www.ijiarec.com

ISSN:2348-2079 Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Monitoring and Prevention of Stealthy Denial of Service Strategy

[1]Mr. C. Mani M.C.A., M.Phil., M.E., Associate Professor,
[2]Mr. T. Ajith Kumar Final MCA .,
Department of MCA , Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: cmanimca@gmail.com, rithiajith@gmail.com

***Abstract* -Cloud Computing is an emerging paradigm that allows customers to obtain cloud resources and services according to their demand. Service level agreements (SLA) regulate the costs that the cloud customers have to pay for the provided quality of service (QoS).The success of the cloud computing paradigm is mainly due to its on-demand, pay-by-use and self-service nature. According to this standard, the effects of Denial of Service (DoS) attacks involve not only the quality of the delivered service, but also the service maintenance costs in terms of resource usage. Specifically, if the detection delay is longer, the cost will be more. Therefore, a particular attention has to be paid for stealthy Denial of Service attacks. They aim at minimizing their visibility, and at the same time, they can be as harmful as the brute-force attacks. They are sophisticated attacks tailored to leverage the worst-case performance of the target system through specific periodic, pulsing, and low-rate traffic patterns. In this study, a strategy is proposed to orchestrate stealthy attack patterns, which exhibit a slowly-increasing-intensity trend designed to inflict the maximum financial cost to the cloud customer, while respecting the job size and the service arrival rate imposed by the detection mechanisms. Here both how to apply the proposed strategy, and its effects on the target system deployed in the cloud is described.**

***Keywords*— Classification, Cloud computing, DDoS attacks ,LS-SVM.**

I. INTRODUCTION

Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e. the password which is something you 'know', this is sometimes termed one factor authentication. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware.

An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high level analysis. A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria. The most basic protection a firewall provides is the ability to block network traffic to certain destinations. This includes both IP addresses and particular network service ports.

A site that wishes to provide external access to a web server can restrict all traffic to port 80 (the standard http port). Usually this restriction will only be applied for traffic originating from the un-trusted side. Traffic from the trusted side is not restricted.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack)[1] is an attempt to make a computer resource unavailable to its intended users. Although the targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently, that may be temporarily or indefinitely.

Denial-of-service attacks are designed to shut down or render inoperable a system or network. The goal of the denial-of-service attack is not to gain access or information but to make a network or system unavailable for use by other users. It is called a denial-of-service attack, because the end result is to deny legitimate users access to network services. Such attacks are often used to exact revenge or to punish some individual or entity for some perceived slight or injustice. Unlike real hacking, denial-of-service attacks do not require a great deal of experience, skill, or intelligence to succeed.

Committers of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target(victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

The thesis aims to protect DDOS attack day to day issues in the server. The administrator had all privileges to access this website. The administrator logins to the web site protect from the hackers and also DDOS attack. All the denied attacks are blocked the corresponding IP address in the server. It is easy to be made through online by clerks of the concern.

The web is a complicated referral graph, in which a node (website) refers its visitors to others through hyperlinks. They propose to use this graph as a resilient infrastructure to defend against distributed denial-of-service (DDoS) attacks that plague websites today. Suppose eBay allows its trusted neighbors (websites linking to it) such as PayPal to refer legitimate clients to its privileged service through a privileged referral channel.

II.RELATED WORKS

In the paper “WRAPS: Denial-of-Service Defense through Web Referrals” by XiaoFeng Wang and Michael K. Reiter. The web is a complicated graph, with millions of web-sites interlinked together. In this paper, they proposed to use this web site graph structure to mitigate flooding attacks on a website, using new web referral architecture for privileged service (“WRAPS”).

WRAPS allows a legitimate client to obtain a privilege URL through a click on a referral hyperlink, from a website trusted by the target website. Using that URL(Uniform Resource Allocator), the client can get privileged access to the target web- site in a manner that is far less vulnerable to a DDoS(Distributed Denial of Service)flooding attack. WRAPS does not require changes to web client software and is extremely lightweight for referrer websites, which eases its deployment.

In the paper “CAPTCHA: Using Hard AI (Artificial Intelligence) Problems For Security”. They introduce captcha, an automated test that humans can pass, but current computer programs can't pass: any program that has high success over a captcha can be used to solve an unsolved Artificial Intelligence problem. They provide several novel constructions of captchas.

Since captchas have many applications in practical security, user approach introduces a new class of hard problems that can be exploited for security purposes. Much like research in cryptography has had a positive impact on algorithms for factoring and discrete log. A Captcha is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs can't pass

In this paper “Preventing Internet Denial-of-Service with Capabilities”, by Tom Anderson Timothy Roscoe and David Wetherall. In this paper, they proposed a new approach to preventing and constraining denial-of-service attacks.

Instead of being able to send anything to anyone at any time, in user architecture, nodes must first obtain “permission to send” from the destination; a receiver provides tokens, or capabilities, to those senders whose traffic it agrees to accept.

The senders then include these tokens in packets. This enables verification points distributed around the network to check that traffic has been certified as legitimate by both endpoints and the path in between, and to cleanly discard unauthorized traffic. They show that user approach addresses many of the limitations of the currently popular approaches to DoS based on anomaly detection, traceback, and push back.

In this Paper “Implementing Pushback: Router-Based Defense Against DDoS Attacks” by John Ioannidis and Steven M. Bellovin, Pushback is a mechanism for defending against distributed denial-of-service attacks.

DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not obeying traditional end-to-end congestion control, the problem must be handled by the routers.

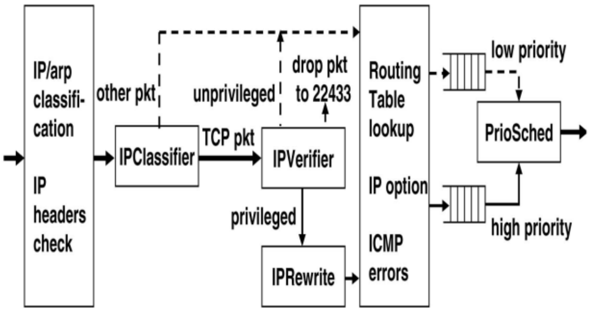
Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack. Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router’s resources be used to route legitimate traffic. In this paper, they present an architecture for Pushback, its implementation under FreeBSD, and suggestions for how such a system can be implemented in core routers.

In this Paper “Promoting the Use of End-to-End Congestion Control in the Internet” by Sally Floyd and Kevin Fall, This paper considers the potentially negative impacts of an increasing deployment of non-congestion-controlled best-effort traffic on the Internet. These negative impacts range from extreme unfairness against competing TCP (Transmission Control Protocol) traffic to the potential for congestion collapse.

To promote the inclusion of end-to-end congestion control in the design of future protocols using best-effort traffic, they argue that router mechanisms are needed to identify and restrict the bandwidth of selected high bandwidth best-effort flows in times of congestion. The paper discusses several general approaches for identifying those flows suitable for bandwidth regulation.

III. METHODOLOGY

- Receive a request.
- Check IP Address in blocked list.
- Check Requested URL of importance against attack. i.e., the document or web page is required to be checked for attack.
- If the count of requests is found to be reached to allowed limit in a specified period, then redirect the request to access denied page
- The last request time is stored again so that the successive requests' time are checked for request count.



A. ALGORITHM IMPLEMENTATION OF ATTACK

In this module, the proposed attack strategy, namely Slowly-Increasing-Polymorphic DDoS Attack Strategy (SIPDAS) is applied. It leverages known application vulnerabilities, in order to degrade the service provided by the target application server running in the cloud.

The term polymorphic is inspired to polymorphic attacks which change message sequence at every successive infection in order to evade signature detection mechanisms. The attack is performed until it is either detected.

B. IPADDRESS BLOCKING

In this module, the clients IPAddress details to be blocked are added in back end table. Any IPAddress can be added or removed at any time. During addition, listening this address for all page requests or particular page request is selected. If particular page, then page URL is given. The minimum number of request count and time is entered so that only after that limit is reached, the request is redirected.

IPClassifier classifies all inbound packets into three categories: packets addressing the website's privilege port which are dropped, TCP packets which are forwarded to IPVerifier, and other packets, such as UDP and ICMP, which are forwarded to the normal forwarding path.

C. RESOURCES SETTINGS TO BE MONITORED FOR DDOS ATTACK

In this module, the source web pages such as html or aspx page are entered. In addition, image files such as jpg or gif files path is entered so that they can be listened for attacks.Therefore, supposing that mRð#kÞ and sRð#kÞ are the mean and standard deviation of the response time tR for the messages type #k, empirically estimated during the training phase, the Meter can adopt the following Chebyshev's inequality to compute deviation of the service time tSð'iÞ during the attack:

$$p(|t_S(\varphi_i) - \mu_R(\vartheta_k)| \geq \lambda * \sigma_R(\vartheta_k)) \leq \frac{1}{\lambda^2} \quad with \quad \varphi_i \in \vartheta_k.$$

D. MONITOR AND PREVENT THE DDOS

In this module, the global.asax (Active Server Application) page is written with attack listening coding. The requested client URL's IPAddress is checked whether it is blocked. If that particular client is requesting more than given specified times with in given time period.

In this module, attack prevention coding is written such that requested client URL's IPAddress is checked whether it is blocked. If that particular client is requesting more than given specified times with in given time period then it is redirected to accessdenied.aspx page.

E. REQUEST LOG AND CAPTCHA FORM

In this module, the requests made by clients are saved for future analysis. The records are displayed using GridView control which is bind through DataAdapter.

In this module, a web page is designed with CAPTCHA form, in which, the mathematical equation is randomly generated and after solving the equation, the required web page is navigated.

IPVerifier verifies every TCP packet's capability token embedded in the last octet of the destination IP address and the 2-octet destination port number. Verification of a packet invokes the MAC over a 5-byte input and a 64-bit secret key. The packets carrying correct capability tokens are sent to IPRewrite, which sets a packet's destination IP to that of the target website and destination port to port. WRAPS overcome the drawbacks through checking the HTTP_REFERER property in Request. If the value is null, it is clear that the page is requested programmatically by an application.

In this module, a web request is checked such that the router application receives the request, process the query string information, the ip address parsing work done and the request is authenticated.

IV. CONCLUSION

The Secure Overlay Service system needs to increase the server speeds or number of servers to balance the client's request. DDoS attack is a critical threat to current Internet. Recently too many technologies of the detection and prevention have developed, but it is difficult that the IDS distinguishes normal traffic from the DDoS attack.

The DoS threats could be mitigated through exploring the enormous interlink age relationshIPs among the websites themselves. The design and implementation of WRAPS, a web referral infrastructure for privileged service, and empirically evaluated its performance. WRAPS enables clients to evade very intensive flooding attacks

Thus the automated generated code, which is unique for each message is attached and sent. The administrator verifies the code and checks the IP address details when there is a mistrusted user. The hacker users were requested to provide the authentic details and those details are verified with the interfaces connected to the server.

When the user did not use the service for a long period, then the user was removed based on the proposed system. Denial-of-service attacks are designed to shut down or render inoperable a system or network.The goal of the denial-of-service attack is not to gain access or information but to make a network or system unavailable for use by other users.

It is called a denial-of-service attack, because the end result is to deny legitimate users access to network services. Such attacks are often used to exact revenge or to punish some individual or entity for some perceived slight or injustice. Unlike real hacking, denial-of-service attacks do not require a great deal of experience, skill, or intelligence to succeed. Committers of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management.

REFERENCES

[1] X. Wang and M. Reiter, "Wraps: Denial-of-Service Defense through Web Referrals," Proc. 25th IEEE Symp. Reliable Distributed Systems (SRDS), 2006.

[2] L. von Ahn, M. Blum, N.J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," Advances in Cryptology—EUROCRYPT '03. SpringerVerlag, 2003.

[3] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing Internet Denial-of-Service with Capabilities," Proc. Second Workshop Hot Topics in Networks (HotNets '03), Nov. 2003.

[4] J. Ioannidis and S. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks," Proc. Symp. Network and Distributed System Security (NDSS), 2002.

[5] S. Floyd and K. Fall, "Promoting the Use of End-to-End ongestion Control in the Internet," IEEE/ACM Trans. Networking, Aug. 1999.