Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of Application Layer Denial of Service Attacks and Detection Mechanisms

Shazia Shafi*, Sanjay Jamwal
Department of Computer Science
Baba Ghulam Shah Badshah University,
Rajouri, J&K, India

Abstract— In the world of internet denial of service attacks are becoming very common. These attacks are increasing with the great pace and have increased the risk of network devices and servers than before. Denial of service attacks have become a serious threat in the internet security. In these attacks, the attacker in a short span of time sends a large data to the server which does not make the service available to the legitimate users. Application Denial of Service attack is a new type of attacks. It exploit the flaws either in implementation or the design of the application. These attacks are done easily but are harder to get detected. A large amount of work has been done on the detection of application Denial of Service attacks. In this paper, we present different types of Application Layer Denial of Service Attacks and review their detection mechanism. The main aim of this paper is to cover the major aspects of detecting the Distributed Denial of Service Attacks. Here we provide review of different papers that describe the methods of detection of the Application Layer Denial of Service Attacks.

Keywords— Application Layer Denial of Service Attacks, Denial of Service Attacks, DDOS, Data Flood Attack, Protocol Feature Attack.

I. INTRODUCTION

In recent world DOS attacks are becoming prominent in the internet world. These attacks are increasing with the great pace and have increased the risk of network devices and servers than before. Due to this reason people and organisations that are having data and large servers on the internet are making great investments and plans to defend themselves and make their data secure against different attacks which also includes Denial of Service Attacks. According to Prolexic survey there is 22%increase in the DOS attack. Q3 of 2014 them that of Q2. It has been found that on an average 28 attacks are performed in a day. The attacks mainly target the hardware resources, bandwidth and the services provided to the users [1]. These attacks are very simple but are very powerful attack the internet resources. The attackers quickly launch the attacks as the architecture of World Wide Web is prone to many types of threats which also includes Denial of Service Attacks and they have various automated tools available for launching the attack which require less human effort. The main aim of the attack is to degrade the services by sending large traffic to the legitimate user. The main property which makes them powerful is that these attacks are harder to get detected as these attacks show legitimate behaviour. There are many reasons for an attacker to launch an attack on any system. Some reasons may be [2]:

A. Revenge:

Revenge is the most frequent and most common reason for launching a DOS attacks .Dispute with any person be it a friend, ex-employee or any customer may lead them to have a motive for an attack. The reason for launching a new attack may be any major issue or minor disagreement.

B. Hiding illegal activities

Sometimes DOS attacks are used by some attackers to divert the attention of the victim so as to hide other illegal activities.

C. Politics

In politics DOS attacks are used by the groups or by terrorist to launch an attack so as to silence the opposition dignity.

D. War

In today's world government are now trying to develop potentials for the cyber war in which the DOS attacks can be used as a tool for attack.

E. Challenges

Sometimes many people want to show their intellectual capabilities by launching a DOS attack.

II. CLASSIFICATION OF DOS ATTACK

There are various types of DOS attacks. Some of them are [3]

A. Network device level:

In the network device level attack the main target of the attackers are the hardware devices on the network. The attackers launches this type of the attack by exploring some vulnerabilities in the hardware resources or by exploring some software loopholes. Routers and firewalls are affected in this type of attack.

B. Operating system level attack :

In this type of attack the loopholes in the operating system of the target machines are used to perform an attack. End user equipment are the most affected areas in this type of attack.

C. Application level attack :

In this type of attack the loopholes in the application are exploited for launching a DOS attack. This type of attack is most prominent today's world. These types of attacks are becoming harder to get deleted as the traffic behaves same as that of the legitimate traffic. The application level attacks is more successful for the attackers. The most affected areas are the web application.

D. Data flood attackers :

In data flood attacks the main target of the attackers is the bandwidth of network.in this of attack the attackers generates a heavy traffic so as to exhaust all the bandwidth of a network. This degrades the normal services so the legitimate requests are devised. The victim's machine is mostly affected by this type of an attack.

E. Protocol feature attack :

In this type the loophole in certain protocol features are used to explore them for performing a DOS attack. Example is the IP address spoofing in which the IP address is spoofed to launch a DOS attack by an attacker that becomes much harder to get traced due the fake IP address. Client server PCs are the most affected areas.

III. APPLICATION LAYER DOS ATTACKS

In today's world DOS attacks are becoming more powerful and are occurring frequently [14]. DOS attacks are oldest type of attacks on the internet and are considered as one of the most disruptive and intense attack for depleting the computing resource or the bandwidth of the network. As these attacks are trivial in their execution, so these attacks are easily detectable because of their voluminous and dynamic attack rates. So now in the recent years there is a trend of new and more sophisticated attacks known as application layer Denial of service attacks. These attacks have some impact as that of the DOS attack but are more dangerous because they are not easily detected. It is because these attacks show the legitimate behaviour so as to avoid detected. It is that type of attack in which the attacker attacks the particular application and makes service unavailable to the legitimate user.

Application layer DOS attacks most target vulnerabilities and specific characteristics of protocol application layer. Malicious traffic cannot be distinguished from the normal data, it also adopts the automated script to avoid the need of large bandwidth of machines to launch the attack. It is also very difficult to detect the application denial of service attacks due to multiple redirections at the proxy server.

IV. CLASSIFICATION OF APPLICATION LAYER DENIAL OF SERVICE ATTACKS

The application layer DOS attacks are broadly divided into different classes [15]:

A. Request flooding:

In this type of attack the requests to the protocol are sent at the higher rates so as to deplete all the session resources. It enables the web servers to disrupt and degrade the functioning.

B. Asymmetric:

In this type of attack the requests with huge workload are sent at normal rate so as to exhaust the resources of the server.

C. Hybrid:

It is actually the combination of the request flooding and attacks the asymmetric attacks. In this type of attack the requests with huge workload are sent at higher rates.

There are two other categories of Application Layer DOS attacks which are slow rate and Low rate attacks.

D. Low rate attacks:

Low rate attack is the modified and intelligent version of the DOS attack. Its main aim is to send the packets that seem like the legitimate one at a low rate so as to avoid detection. It leads to the exhaustion of the resources and makes service unavailable to the users. It is difficult to detect and mitigate this type of attack.

E. Slow rate attacks:

Slow rate attacks, transmit the packets at a same speed so as to avoid the detection. One of the common properties of the application layer protocol is being exploited by slow rate DOS attacks. It transmits the data at the low pace so as to allow the attack to deplete the resources of the server that cause the denial -of-service attacks.

Application layer DDOS attacks need to establish the TCP connection with the victim computer. So an attacker needs to reveal the real IP of the systems to the target machines else the connection cannot be completed. As the attackers uses a large number of system so this limitation is not a worthy for the attacker [13]. If the packets of such machines are filtered and identified the attacker doesn't work as it uses another group of zombie computers to launch an attack. After the connection is completed with victim computer the attacker sends requests so as to start the communication.

V. APPLICATION LAYER DOS ATTACK DETECTION MECHANISMS

The most popular type of attack in today's networking world is the Application Layer Denial of Service attack. In Application Layer Denial of Service attacks the attackers try to create a TCP connection with a victim computer and after that floods the requests so as to bring the victim system down. This helps them in concealing their identity so as to escape from the methods for detection. Many of the mechanisms of detection are used to recognize the attacks of network layer. So application layer attacks have become more fruitful to the attackers so as to attack victims. There has been a good contribution of researchers in identifying the DOS attacks by the inspection of traffic behaviours that occur due to the traffic flow based on attack efforts. The most vital task for this context is to make a difference between the attack and a flash crowd. If there is a sudden increase in the legitimate connections occurring at a short period on a service or a web site it is known as flash crowd [25]. There have many attempts to detect the DOS attacks. Some of the techniques are used to examine the traffic anomalies so as to detect both the network layer attacks as well as application layer attacks, while as some of them are only focused to protect and against the application layer DOS attacks only. Here are some of the attempts to provide a defence against Application Layer Denial of Service Attacks.

In [27] they proposed a techniques of parametric methods so as to identify the anomalies in the network data flow by using the aggregate of traffic properties where no flow separation is used. This method is known as bivariate Parametric Detection Mechanism (bPDM). It makes the use of the probability ratio of the packet size and the traffic rate statistics. Bit rate Signal to Noise Ratio (SNR) metric is used to detect the network abnormality and validate it by analysing bPDM with bit rate SNR in different three environment which is also include a real time DOS attack. They were capable of detecting different attacks within few second only [28]. It was also found that there is decrease in the detection as there is increaser in the bit-rate SNR value. Also with the increase in rate of attacks, the time detection decreases.

In [26], author has proposed a discovery of DOS attacks by monitoring the network. They have found that when a DOS attack strikes there has been the shift in the spatial-temporal patterns of traffic of the network. These effects were tested with many attack modes like increasing rate attacks, constant rate attack and pulsing attack. Results obtained after the simulation show that change in the spatial- temporal pattern is detected efficiently with little of the facts of observation. By this method the location and the time of attack is also obtained without spotting victim side alterations.

In another research in [29] the authors have discussed the group synchronisation issue that is required by the server for maintenance of the group of clients by using the-hopping method [30]. In some cases where there are clock- rate drifts in many interacting system, here are possibilities in which some control signals may get missed, so the serval port is kept open for more time by which the serval becomes susceptible to the Application Layer DOS Attacks. So they have given an algorithm which is known as BIGWHEEL in there occurs the port-hopping mechanism for communicating the multiple system but there is no need of synchronisation. Also another algorithm known as HOPERAA was also proposed for the execution of the post hopping in the present of clock-rate drifts. It was also found that the group synchronisation raise some scalability issues. In the proposed algorithm, server provides the simple boundary to every client which the post hopping period of a protocol is permanent, so there are very less chances launching on application dos attack at the port of the server [31].

In [33] an attempt has been made by the authors so as to detect the application layer DOS attacks in the web traffic. They have made access matrix that are multidimensional so as to get the spatial temporal patterns of flash crowd and also introduced a method that was based a document popularity [34].The access matrix is actually abstracted but the component analysis of flow of traffic [35] and the document popularity that was used was obtained from the log of the server. They have devised a detector based on huddler semi Morkov Model [36] that was used for the detection of anomaly in the traffic of the network. The detector proposed was used to describe the matrix dynamics and to detect the DOS attacks. They experimented the application DOS attacks during the flash crowd event in real time and the obtained data was used in the detector proposed. The result obtained explained that model can detect the Application DOS attack by making the use of document popularity.

In [32], the author has made an attempt to distinguish between DOS attacks and flash crowd by making the use of hybrid probability metric. The nature of the application layer DOS attacks and flash crowd is same but there are some differences in access dynamics, traffic rates and source IP address distribiution.by using these differences, the authors have devised that distinguished flash crowds for the DDOS packets .in that algorithm their basic work was based on the flows of traffic and they examined abnormalities by siting two different grouping threshold to similarity index and variation. On the basis of the variation of any distributions calculated and then comparing with the given threshold, they distinguished DOS packets from crowds.

In [37] the authors proposed a mechanism to defy Application Layer DOS attack known as shield. This mechanism is composed of two components, one is the DDOS Resilient Scheduler [38] and the second is the suspicious assignment

mechanism. They have picked up few specific properties of attack that are based on the session. Some of them are request flooding and asymmetric workload so as to detect Application Layer Attacks. Bases on such properties, the suspicious assignment mechanism gives a value that is continuous (not binary) to the session as per its deviation to given behaviour and use the DDOS resilient schedule to find if the session is to be processed. To determine the efficiency of proposed mechanism they make use of a new test to the web application that was hosted. As per the results obtained it was found that DDOS shield improves the performance of victim computer significantly if there is an attack with symmetric workload so as to exhaust resources of the server.

VI. CONCLUSIONS

In this paper, we presented a review of Application Layer Denial of Service Attacks and some of the defense and detection techniques. The major challenge identified in this research is that the application layer Denial of Service Attacks are harder to get detected. It is because in application layer Denial of Service Attacks the malicious traffic behaves same like that of the legitimate traffic, so it avoids the detection. Therefore, the future research in this field is even more challenging.

REFERENCES

[1] Jovi D Silva, Kukatlapalli Pradeep kumar, and Balachandran K, "Studies of Prominent DDOS Attacks in the Internet: their Causes, Preventions and Causes Studies", *International Journal of Computer Science Engineering and Information Technology Research* Vol. 4, Issue 3, June 2014.

[2] Rajkumar, Manisha Jitendra New, "A Survey on Latest DOS Attacks: Classification and Defense Mechanisms", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 1, issue 8, Oct 2013.

[3] M. Aamir and M. A. Zaidi, "A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques," *Interdisciplinary Information Sciences*, vol. 19, no. 2, pp. 173-200, November 2013.

[4] G.-L. S. A. A. G. Hugo Gonzalez, "The Impact of Application Layer Denial of Service Attacks," *Information Security Centre of Excellence*, University of New Brunswick, 2013.

[5] Arbor Networks (2012). The growing threat of application-layer DDOS attacks.

[6] H. Beitollahi, and G. Deconinck, "Denial of Service Attacks: A Tutorial", *Electrical Engineering Department (ESAT), University of Leuven*, Technical Report: 08-2011-0115, August 2011.

[7] I. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. E. Long, "Managing flash crowds on the Internet," *In Proc. of 11th IEEE/ACM Intl' Symposium On Modeling, Analysis and Simulation of Computer Telecommunications Systems (MASCOTS), IEEE/ACM*, pp. 246-249, October 2003.

[8] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," *IEEE/ACM Transactions on Networking*, vol. 19, no. 2, pp. 512-525, April 2011.

[9] X. He, C. Papadopoulos, J. Heidemann, U. Mitra, and U. Riaz, "Remote detection of bottleneck links using spectral and statistical methods," *Computer Networks, Elsevier*, vol. 53, issue 3, pp. 279-298, February 2009.

[10] J. Yuan, and K. Mills, "Monitoring the Macroscopic Effect of DDoS Flooding Attacks," *IEEE Transactions On Dependable and Secure Computing*, vol. 2, no. 4, pp. 324-335, October 2005.

[11] Z. Fu, M. Papatriantafilou, and P. Tsigas, "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts," *IEEE Transactions On Dependable and Secure Computing*, vol. 9, no. 3, pp. 401-413, May 2012.

[12] K. Hari, and T. Dohi, "Sensitivity Analysis of Random Port Hopping," *In Proc. of 7th Intl' Conference On Ubiquitous Intelligence & Computing and 7th Intl' Conference On Autonomic & Trusted Computing (UIC/ATC), IEEE*, pp. 316-321, October 2010.

[13] G. Badishi, A. Herzberg, and I. Keidar, "Keeping Denial-of-Service Attackers in the Dark," *IEEE Transactions On Dependable and Secure Computing*, vol. 4, no. 3, pp. 191-204, July 2007.

[14] Y. Xie, and S. Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," *IEEE/ACM Transactions On Networking*, vol. 17, no. 1, pp. 15-25, February 2009.

[15] S. A. Krashakov, A. B. Teslyuk, and L. N. Shchur, "On the universality of rank distributions of website popularity," *Computer Networks, Elsevier*, vol. 50, issue 11, pp. 1769-1780, August 2006.

[16] J. Shlens, "A Tutorial on Principal Component Analysis," ver. 3.01, < http://sloan-swartz.salk.edu/shlens/pca.pdf>, April 2009.

[17] Y. Xie, and S. Z. Yu, "A Novel Model for Detecting Application Layer DDoS Attacks," *In Proc. of 1st Intl' Multi-Symposiums on Computer and Computational Sciences (IMSCCS '06), IEEE,* pp. 56-63, June 2006.

[18] K. Li, W. Zhou, P. Li, J. Hai, and J. Liu, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics," *In Proc. of 3rd Intl' Conference On Network and System Security (NSS '09), IEEE*, pp. 9- 17, October 2009.

[19] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly, "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks," *IEEE/ACM Transactions On Networking*, vol. 17, no. 1, pp. 26-39, February 2009.

[20] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDoS Resilient Scheduling to Counter Application Layer Attacks Under Imperfect Detection," *In Proc. of 25th Intl' Conference On Computer Communications (INFOCOM), IEEE*, pp. 1-13, April 2006.

