ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

A Survey: Software Puzzle- A Countermeasure to Resource Inflated Denial of Service Attacks.

K Rajkumar*,P Swaminathan and R Sheeba.

Computer Science & Engineering, School of Computing, SASTRA University, Tirumalaisamudram, Thanjavur-613401,Tamilnadu, India.

ABSTRACT

Denial-of-service (DoS) and distributed denial of service (DDoS) are the main threats in the cyber security to deny these attack many techniques has been introduced some of the techniques are related to cryptographic and some of them is based on web application[1][4]. Based on these many techniques has been introduced some of the techniques is more secure but not interoperable and some provide reliability but it is not secure so to find the features in these techniques survey is created. In this survey paper several techniques has been analyzed and the best method is examined to avoid the DoS attack.

Keywords: Software Puzzle, One-time-Password, Distributed-Denial-of-Service.

Corresponding author

INTRODUCTION

Denial of service is a kind of attack on a network which is sketched to escort the network down by immerse it with unwanted traffic and Distributed denial of service attack is one in which abundance of computer system attack a single target[2][7]. These both type of attack will decrease online resources such as network bandwidth, memory & computation power by devastating the service with malicious request. For example a malicious client send many number of garbage request to, HTTPS bank server on the other side the server has to spend much time for these request this results in wastage of more CPU time and finally the server doesn't have efficient resources to serve the client request [3].In this case the attacker spend little effort to send the request to server but on other hand server need more effort to solve these handshake and the quality of service will be degraded [5].

The existing techniques available is of generally two type one is avoiding the DoS attack using the web application and another one is by using cryptographic function .Both of them avoid these kind of attack but the puzzle technique will be more interoperable than the cryptographic technique but the cryptographic function will use several advance encryption technique to avoid malicious request. In the web based technique captcha, puzzle, time lock is used to avoid the attacks. In below several techniques has been compared and the features has been analyzed for avoiding the DoS attack [6][7].

CLASSIFICATION OF DoS ATTACK:

DoS Resistant Authentication: It uses the authentication protocol that is server first authenticate then it allocates the resource for the client. Before allocating the client should commit it own resources .The DoS attack is prevented by increasing the client cost the one way to increase the client cost is to create puzzle and the puzzle should be solved by client using brute force technique or one way hash function these method will complicate the client puzzle once the puzzle is solved along with the puzzle solution the resources it needed is also send to the server. The server verifies the solution if it is correct then server will allocate the committed resources otherwise it will deny the request this method will avoid resource depletion and the bandwidth is also not wasted[5].

Sample Processing Algorithm: It is used to mitigate DoS attack. The sample processing algorithm is initiated only at the time of congestion the congestion is notified by use of alarms if traffic exceed the particular limit the alarm signal will be send to router indicating congestion. Once the router congested first it use random early detection (RED) algorithm to decide whether to present the packet in a queue or to drop the packet if packet is dropped it is taken into congestion triggered packet sampling in this all these dropped packet take available token and then it is processed by a sample processor. If token is not available then packet is discarded. In this approach the samples are treated immediately at the initial stage to detect DoS attack [4][8].
Path Identification: The DoS attack is reduced by the path identification mechanism that is each packet has unique path and unique identifier by using this we are filtering the denial of service attack. The existing trackback mechanism will reconstruct the path in the router this technique will be more complex thus new technique called path marking scheme has been developed in this each packet has unique path thus different marking the malicious client transmit all the packet in the same path thus it has same marking[9]. The packet with same marking is filtered by the adaptive filters at the router so that the traffic is regulated and the resource depletion at the server side is avoided.

Proof of Work Scheme: In this method for each client the challenge will be given by the server this challenge act as a filter the difficulty of a challenge is based on their load. The client past load and the current load is measured based on this the challenge will be assign. If the client load is higher then the work function will be higher if client load is smaller then the work function will be small. Server issues work function the client solves it and solution is send to the server for verification if it is valid then the request is proceeded otherwise the server will deny the request the increase use of proof of work scheme will reduce DoS attack and also support transparency and backward compatibility for legacy client[6][10].

Active Network Power Defense Mechanism: To defend against DoS attack the new technique Aegis has been used. In the conventional approach once the attack has happen the router will be congested then the firewall will remove all the malicious user and allow only the legitimate user to access the server. In this method the simple firewall will only process the packet thus bandwidth is utilized larger sometime it may also block the legitimate client to access the server. To avoid this aegis has been used in this approach it use a distributed firewall at multiple optimal location to block the unwanted packet. The Aegis is easy to implemented and it is present at the upstream of active network thus bandwidth is consumed less and the congestion is also reduced at the router[2][5][11].

Attack Detection Using Cluster Analysis: It is a proactive method of detecting the DoS attack In this attack is identified at the early stage by analyzing the cluster. In this method based on the feature the traffic parameter is examined then all these parameter is combined to form the groups or cluster to examine the traffic. Each cluster has particular entropy value these entropy resembles the particular phases of DoS attack the phases may be normal, phase 1, phase 2 & attacked state. All these state is decided based on the cluster formation this approach is easily implemented since it use only the normalized distance value and the traffic feature help to build a defense mechanism against distributed denial of service attack.

Cryptography based DoSAttack: In this they have used a cryptographic client puzzle to reduce the connection depletion attack. In this method when the server does not have any evidence on attack it will accept the connection in a normal way .If the server find the attack then it will not accept all the connection it will accept the connection in a selective manner the selection is based on the client puzzle technique that is server will send a cryptographic puzzle that is puzzle is built by combining the small puzzle it is delivered to the client. The legitimate client solve the puzzle within the given time period but the attacker takes more time to solve the puzzle after solving the solution to puzzle is sent to the server for verification if the puzzle is correct and solved within the time period then only that connection is accepted the client which is not able to solve within the period is rejected[12].

PTCP: In this approach they use PTCP that is puzzle at TCP (Transport layer) for preventing POS attack. The transport layer is used for internet connection and other activities thus have build in TCP. In the PTCP the server receive a packet SYN and replies with ACK. If the server examine more traffic in SYN queue .The server send a nonce and difficult level to client, the client solve the puzzle and send solution to server the server works and establish a connection. The nonce 60 sec for client, the difficult level is set up based on the clients load the PTCP puzzle is built based on the block cipher[10].The client solves the puzzle in fast manner by using XTEA6 encryption algorithm. The PTCP is backward compactable, simple and is used in all embedded devices.

Push Back Scheme: In this work the DDoS attack is treated as congestion and the objective is to reduce congestion for this they have used push back technique. This is implemented inside the router the each router will find the traffic and classify into two types that is Good traffic and Bad Traffic. The good traffic will reach the destination and it will not match the congestion signature. The bad traffic is the one will match the congestion signature. The packets in the Bad traffic is dropped and send to push back daemon. This will periodically update the rate limiter parameter and their upstream to be updated [7].

DoS Attack with Puzzle Auction: The new scheme called puzzle auction is implemented to reduce DDoS attack. In this approach client sent the request first to the server as more traffic then it will discard the request, if there is more traffic the request is processed by the server. If it is discarded client will solve the puzzle then it will re-transmit the puzzle solution with the request to the server, if the server is free it will be proceeded else will be discarded, if the request is again discarded the client will increase the difficulty and solve the puzzle then the puzzle solution is sent to the server. If the server is free it will be proceeded else discarded. The retransmitted and bidding strategy goes on increasing until it wins. Since the server treats the priority packet, first the bidding scheme will increase the difficulty until it wins. This technique is more compatible, interoperable and this is implemented in TCP [4][9].

Feedback Mechanism of Filtering: This mechanism has been employed in diff server at the ingress router to reduce the DDoS attack. In this the differentiated servers recognize the prescribed client and its QOS. The client is identified by the packet signature this signature comprises of source address and IP address. Since the malicious client can easily hack the source address these address keep on changing at a fixed interval and at faster rate so that the duplication will be avoided by the attacker this feedback mechanism does not use any cryptographic measure to detect DoS attack. This method is simple and easily implemented at the ingress router[5].

Xeno Service: The DoS attack is avoided with use of Xeno service the Xeno service contain Xeno server this should be installed by all internet service provider at the lower rate. The website under Xeno server should be dynamic replicated to other Xeno server then the bottleneck is avoided by the use of distributed domain name service. The host which is attacked need the additional capacity from the Xeno server this fluctuation in the capacity is notified and filtering is done to avoid DoS attack[3]. At the time of filtering the replicated domain name service at the other Xeno server will provide the service to the customer.

Graphic Turing Test: In this the DoS attack is reduced by using web SOS(Secure Overlay Service) .In this the SOS architecture the target is protected by the attacker by using high performance router and the adaptive filter this will block all the node that are not approved the node which are all approved it should be kept secret or unknown from the attacker . This form the secure overlay any transmission that wish to cross across the overlay should pass the graphic Turing test. The graphic turing test is a visual test the CAPTCHA will be shown in a distorted image the human can easily read the CAPTCHA but the automated system cannot this differentiation make the human to pass the test and fails the automated system.

Max-Min Fair Server Centric Router Throttles: The max-min fair scheme is developed on server centric router for aggressive DoS attack. In this router throttle is used for max-min fair scheme if the server load is below the limit then the throttle value is increased if the server load is above the limit the attack is present thus the throttle is reduced this in turn reduce or drop the packet thereby reduce the DoS Attack . The router throttle is more efficient technique it uses less memory and less computing power.

Time Lock Puzzle: In this method the puzzle once it encrypted cannot able to decrypted until the time period expires. The puzzle cannot be solved by the sender also for the given time interval. If puzzle time period is 2 month it should start computing at the initial level to find the solution if it has started at the last 30 days then the puzzle cannot be solved once the time period expires the key will be released for decryption .This method provide more security but it consume more memory and computing power.

CONCLUSION

In this work several techniques has been analyzed to avoid DoS attacks. As the attack increases the resource will be degraded and the server performance will be decreases to avoid these attacks addition to these techniques new techniques also should be added so that the computational cost will be increased and the attacker effect will be decreased. The above comparison denote that different method provide different features like code obfuscation, interoperability and reliability new technique should be created to support all these features and to avoid DoS attacks.

REFERENCES

[1] Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng. IEEE transactions on information forensics and security. 2015; 10(1):168-177.

[2] Ms.E.Kalaikavitha, Mrs. Juliana gnanaselvi. International Journal Of Engineering And Science. 2013;2(10):14-17.

[3] KeunsooLee, Juhyun Kim, Ki HoonKwon, Younggoo Han, Sehun Kim. ACM Expert Systems with Applications.2008; 34(3):1659–1665.

[4] JelenaMirkovicand Peter Reiher. IEEE Transactions on Dependable and Secure Computing. 2005; 2(3):216-232.

[5] D. K. Y. Yau , West Lafayette, J. C. S. Lui, Feng Liang. ACM Transaction on Networking. 2005; 13(1):29-42.

[6] Yih Huang J. Mark Pullen. Countering Denial-of-Service Attacks Using Congestion Triggered Packet Sampling and Filtering. International Conference on Communications and Networks. 2001; 490-494

[7] A framework for password-based authenticated key exchange. ACM Transactions on Information and System Security. 2006; 9(2): 181-234

[8] William G. MoreinAngelos ,StavrouDebra L. CookAngelos ,D. KeromytisVishal Misra. Using Graphic Turing Tests To Counter Automated DDoS Attacks Against Web Servers. Proceedings of 10th ACM conference on Computer and communications security.2003; 8-19.

[9] T. J. McNevin, J.-M. Park, R. Marchany. pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks. Virginia Tech Univ., Dept. Elect. Comput. Eng., Blacksburg, VA, USA, Tech. Rep. TR-ECE-04-10. 2004; 1-15.

[10] Y. I. Jerschow, M. Mauve. Non- parallelizable and non-interactive client puzzles from modular square roots. Int. Conf. Availabil- ity, Rel. Secur. , 2011; 135-142.

[11] X. Wang, M. K. Reiter. Mitigating bandwidth-exhaustion attacks using congestion puzzles. 11th ACM Conf. Computer Communication Security. 2004; 257–267.

[12] H.-Y. Tsai, Y.-L. Huang, D. Wagner. IEEE Trans. Inf. Forensics Security. 2009; 4(2): 257–267.