Enhancing Security by Preventing DoS and DDoS Attack using Hybrid Approach

R. Sheeba* and K. Rajkumar

School of Computing, SASTRA University, Thirumalaisamudram, Thanjavur - 613401, Tamilnadu, India; Sheebaramesh123@gmail.com, Rajkumar@cse.sastra.edu

Abstract

Objectives: Denial-of-service (DoS) and distributed-denial-of-service (DDoS) are the critical threats in the network security. To overcome from these kinds of attacks the existing system created a puzzle scheme called software puzzle. However the malicious user tries to solve the puzzle, the graphics processing unit (GPU) which is present inside the computer will decrease the effect of the client puzzle. Methods: In this method the puzzle algorithm is generated randomly based on the client request. Once the request is received the server will generate the puzzle with random key, the client receive the puzzle process it and generate the solution for the puzzle. The server verifies it. The drawback in the existing system is that the puzzle does not contain time period so the attacker will hack the key at any time and flood server with malicious request another one is that As the DDOS attack increases, the puzzle difficulty should be also increased, Increase in difficult level the computation cost also increases. Findings: To overcome from this the proposed method contain encrypted one time password (OTP) that is server will generate encrypted OTP based on the Hash function and the salt it is send to the client, Then the client will decrypt the OTP. Based on the decrypted value the client will type the password and send to the server, it will check the password with the mapped value. Another advantage in the proposed method is that it only allow three time for each user to enter wrong password in fourth time the puzzle will be generated the user has to solve and the server will check it. The puzzle solving is created to check whether it is a malicious user or a genuine client by this security is improved and denial of service attack is reduced. Applications: In this approach website security is increased, Attacker chance of hacking and flooding the server with malicious request will be reduced, Allow only genuine user to access the website by use of encrypted OTP and Puzzle approach.

Keywords: Distributed-Denial-of-Service, Encrypt, Hash Function, One-time-Password, Salt, Software Puzzle

1. Introduction

DoS is a kind of attack on a network which is sketched to escort the network down by immerse it with unwanted traffic and DDoS attack is one in which abundance of computer system attack a single target. These both type of attack will decrease online assests such as network bandwidth, memory, computation power by devastating a service by malicious request. For illustration a vicious client send large garbage request to the bank server on the other side the server have to allocate 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. In this case the attacker spend little effort to send the request to server but other hand server need more effort to solve these handshake and the quality of service degraded. 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

*Author for correspondence

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 existing system the software puzzle¹ is used, in which puzzle algorithm is randomly generated the client has to solve it and the server verifies it the major drawback in existing method is that the attacker can easily flood the server queue with more request. The Proposed Method Contains four design modules that is OTP generation, OTP verification, Puzzle generation and Puzzle verification. In the OTP generation phase the one time password^{2.3} is created with the random value by using the salt algorithm that is random data is added as an extra input to the one-way hash function that "hashes" a secret data, the main function of salts is to fight across the dictionary attacks with a list of secret hashes and also with precompiled rainbow table attack, the value generated is encrypted using secure hash algorithm 256 bit Symmetric key that is similar key is used for both encrypting the data and also for decrypting. Finally it will send to the client through registered mail-id on the other end the client receive the encrypted data and they will decrypt using the advance encryption standard once it is decrypted the client has to map the values this mapping is done using one-way function. In this hashing will catch a variable-size input and finally it changes into fixed-size binary sequence, the client should correctly map the decrypted value with the password.

In proactive⁴ method of detecting the DoS attack. The 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 groups or cluster to examine the traffic. In D-WARD⁵ approach it is implemented in the end router. The main purpose of installing the D-WARD is to monitor the traffic, the D-WARD will monitor the inbound and outbound traffic in the network and it also profile all the forwarded packet source address to provide effective utilization of the bandwidth. In max-min⁶ fair approach the server centric router is used to find the 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 Differentiated servers² method helps to 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 of the user these address have to be 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.

2. System Model

The proposed method is based on encrypted one time password (OTP) that is server will generate encrypted OTP based on the password using the symmetric key cryptography⁸ and it is send to the client, Then the client will decrypt the OTP. Based on the decrypted value the client will type the password and send to the server, it will check the password with the mapped value if both matched then server will process the client request if it is not matched then it will deny the request. The advantage in the proposed method is that it only allow three time for each user to enter wrong password in fourth time the puzzle will be generated the user has to solve and the server will check it. The puzzle solving is created to check whether it is a malicious user or a genuine client by this security is improved and denial of service attack is reduced.

2.1 Proposed Architecture

The Figure 1 describes the way of encrypting and decrypting the OTP. In the first step based on the one-way hash function and the salt algorithm the OTP will be encrypted with the symmetric key² then encrypted value send to the user. The client decrypt the data with the key then based on the decrypted value the user has to type the password if the entered data matched with the mapped value then the user can successfully login if the entered data is mismatched with the original password the puzzle will be



Figure 1. Architecture of Encrypting and Decrypting the One Time Password with the Key.

generated the user has to solve the puzzle and send the solution to the server then it will verifies it if the solution is correct it allow user to login if the puzzle solution is wrong then the client session will be aborted.

2.2 OTP Generation

In this module the OTP will be encrypted and it is send to the client registered mail id. If the user has logging for the first time they should create a new account in the new opening form they should type their passwords and the mail-id. The password should be of 9 characters and the mail-id is used for sending the encrypted OTP once the user registered successfully they can login the first page contain account number and the password if it is correct then the mail will be delivered to the client containing encrypted OTP. The OTP is encrypted by SHA algo-



Information Stored

Figure 2. Description of how the Salt added to the Input.

rithm using 256 bit key in the CBC mode that is plain text is XOR with the initial vector and the obtain result is encrypted with a key to provide the cipher text. As in Figure 2 the chaining will be happens that is cipher text output obtained in the first round is given as input to the second round this cipher text will be XOR with the plain text and encrypted with key to provide new cipher text. The encryption also contain SALT algorithm the main purpose of using salt is to generate more random numbers to the hash function so that it will be difficult for a attacker to break the data.

2.3 OTP Verification

In this phase the encrypted OTP which has been sent to the mail is taken and it is decrypted with the 256 bit key using the SHA algorithm in this from the cipher text the original text will be derived that is from the large size input we are deriving the fixed input value. The decrypted value will be of numbers without exceeding the password size the each password value is mapped using the oneway hash methodology. The decryption will be take place using the CBC mode that is the cipher text obtained will be decrypted with the key and the resulting value will be XOR with the initial vector as a result the plain text will be obtained, then in the next round the next cipher will be decrypted with the key the result obtained will be XOR with the previous cipher like this chaining of computation will be take place to obtain decrypted value. If the decrypted value is 2819 the client has to match the decrypted value with the password that is for 2 they should have to type the value of password for example password is "encrypt12" the text n is in the second part, 1 is in the eighth part, e is in the first part, 2 is in the ninth part so the password will be "n1e2" if this is correct then the server will allow the user to login if the password is not matched the server think as anonymous user and will not serve the client request later the client should start sending the request from the scratch this verification is done to avoid DoS and DDoS attack.

2.4 Puzzle Generation

In this phase the server will generate the puzzle and the client have to find the solution to the puzzle. This phase will be generated only when the password entered in the first login phase goes wrong, if it went wrong the server allow the client to retype the password for another two times that is for genuine client server will allow three valid times to enter the password for all these times if the user has entered the wrong password then the server will generate the puzzle to the client then client has to solve the puzzle, the challenge is given to client is by moving the single tile the user has to join all the number in the correct order this type of puzzle generation occurs to find the malicious user in¹⁰ and to avoid sending more request. In the puzzle solving the puzzle is solved by moving the tile in the adjacent side that is blank slide is moved on all the direction left, right, up, down to obtain the goal state initial the tile are arranged in random manner the goal is to arrange the tile in the ordered manner by moving the blank slide the tiles are arranged the best case in this puzzle solving is finding solution in the less moves the worst case of puzzle solving is having the evaluation function larger value that is solution will be obtained after moving all the tiles.

2.5 Puzzle Verification

As shown In the verification part the puzzle solution is verified by the server once the genuine user solve the puzzle by moving the single tile and make the solution the result will be send to the server by the client. The server will verifies the puzzle if the solved puzzle is correct then the server will allow the client to next phase that is server generate encrypted OTP the user has to decrypt finally match the value and they can login. If the solved puzzle is mismatched the server will treat the user has the malicious client and abort the request. The server will verify each tile position with the solved puzzle tile if it all matched the server will accept the client and process the request if the value not matched it will deny the request then the server will also compute the heuristic function and the evaluation function. This value is computed to find the optimal solution if the optimal solution is not found this resemble the client is malicious one and the server will reject it. The server will accept the client only when the solution is valid if it is correct it will send the request to server queue only when the client has been verified the server will process the client request. If the user has failed the server will drop the request and treat them as vulnerable attacker and will not serve these request these type of verification is done by the server to avoid server depleting all of its resource to unwanted request and to utilize the bandwidth in the efficient way.

3. Experimental Results

In the encrypted OTP method the server will provide guaranteed services to its user that is whenever the user send the request, the backend server generate an encrypted OTP to the client the encryption is done using the SHA algorithm and then random value is added to the encrypted key using salt algorithm. the client receive the encrypted password and they will decrypt it after decrypting the client have to enter the password the server will check the password with the mapped value if it is correct the user will allow client to login if it is wrong client will



Figure 3. Performance Graph showing the reduction of Malicious Request.

reject it and generate the puzzle the user has to solve the puzzle after solving it client has to send the solution to the server it will verifies it if it is valid then server will process the request otherwise server will deny the request. In this approach the password has been strengthen by adding the hash function and the salt and this method also contain puzzle has another gateway of protection thus difficulty level will be increased. As the difficulty level increases the probability of attacker to hack the data will be less. The Figure 3 clearly depicts that request will be increases to 35 if both the encryption and puzzle is not used. If only the puzzle is used then malicious request will be decreased to 25. If both puzzle and encrypted OTP is used malicious request will be reduced to 10.

4. Conclusion

In the network the security is the considered has critical factor, the security is improved in the proposed approach by adding the cryptographic parameter. In this method the password has been strengthen by adding the hash function and the salt. The OTP generated is encrypted with hash function along with the salt and on other side it is decrypted using the key this is usually done to make password more secure and to avoid attacker from hacking the data. The proposed method also contain puzzle has another gateway of protection to increase the difficulty level. As the difficulty level increase the probability of attacker to hack the data will be less by this way the security will be increased and the DoS attack is reduced. In future the biometric parameter can be added as additional parameter to the existing approach so that the security can be increased and DoS attack will be avoided.

5. References

 Yongdong Wu, Zhigang Zhao, Feng Bao, Robert H Deng. Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks. IEEE Transactions on Information forensics and security. 2015 Jan; 10(1):168-77.

- 2. Kalaikavitha E, Juliana Gnanaselvi. Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. International Journal of Engineering and Science. 2013 Apr; 2(10):14-17.
- Jesudoss A, Subramaniam NP. EAM: Architecting Efficient Authentication Model for Internet Security using Image-Based One Time Password Technique. Indian Journal of Science and Technology. 2016 Feb; 9(7):1-8.
- Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim. DDoS attack detection method using cluster analysis. Expert Systems with Applications. 2008 Apr; 34(3):1659–65.
- Mirkovic J, Peter Reiher. D-WARD: A Source-End Defense against Flooding Denial-of-Service Attacks. IEEE Transactions on Dependable and Secure Computing. 2005 Aug; 2(3):216-32.
- 6. Yau DKY, Lui JCS, Feng Liang. Defending against distributed denial-of-service attacks with max-min fair server-centric

router throttles. ACM Transaction on Networking. 2005 Feb; 13(1):29-42.

- Countering Denial-of-Service Attacks Using Congestion Triggered Packet Sampling and Filtering. Date Accessed: 15/10/2001: Available from: http://ieeexplore.ieee.org/doc ument/956309/?reload=true&arnumber=956309.
- Ganesh Kumar K, Arivazhagan D. Generating A Digital Signature Based On New Cryptographic Scheme For User Authentication And Security. Indian Journal of Science and Technology. 2014 Oct; 7(S6):1-5.
- 9. Rosario Gennaro, Yehuda Lindell. Springer Berlin Heidelberg: A framework for password-based authenticated key exchange. 2003 May; p. 524-43.
- William G Morein, Angelos Stavrou, Debra L Cook, Angelos Keromytis, Vishal Misra D. Using Graphic Turing Tests to Counter Automated DDoS Attacks Against Web Servers. Proceedings of 10th ACM conference on Computer and communications security. 2003 Sep; p. 8-19.