Automatic software puzzle generator and Shoulder surfing resistant system to detect and prevent attacks

Khushal Khairnar [1], Radhika Patil [2], AnkitaThakur [2], Prajakta Thakur [2], BhushanWani [2]

Professor, Computer Engineering, MMIT, Maharashtra, India [1]
Student, Computer Engineering, MMIT, Maharashtra, India [2]

ABSTRACT

Network security refers to protecting the network and creating a secure platform for users. In traditional system, users entered text passwords to authenticate themselves which can be easily hacked if someone peeks over their shoulders and if graphical passwords is used then it can be easily remembered by human brains. In DOS attack, the target machine is flooded with continuous dummy request by the DOS attacker so as to overload the system and prevent the request from being fulfilled. Previously a client puzzle was used which demanded the client to solve a puzzle whose algorithm was generated in advance. So the client could solve this puzzle quickly. The proposed system for preventing shoulder surfing attack is shoulder surfing resistant system based on graphical passwords using PassMatrix technique. For DOS attack we are developing a software puzzle which generates the algorithm randomly only after the client request is received by server using puzzle core generation. Hence we will be implementing these two techniques to prevent and detect the attacks.

Keywords :- *Graphical password, Shoulder surfing resistant system, software puzzle, DOS attack, AES(Advance Encryption Standard), OTP(One Time Password).*

1. INTRODUCTION

Nowadays, network security is growing issue as many organizations use the public network for their data, they need to ensure that their data is not accessed by any unauthorized user because without any security measure their data can be subjected to an attack. The attack can be passive in which the information is monitored or it can be active attack in which the information can be modified or altered to corrupt the data or network itself.

In password based attacks like the shoulder surfing attack, the sensitive information of a user, that is the username and password can be hacked when the user authenticates himself in crowded public place. To overcome the vulnerabilities of traditional methods, graphical password schemes has been developed as an alternative solution to text based schemes. Unlike the password based attacks, the Denial of Service attack prevents the normal use of a network by valid users. If the attacker gains access to the network he can flood the entire network by sending invalid data and block the traffic. This results in loss of access to network resources by authorized users.

In this paper we present techniques to prevent the shoulder surfing and DOS attack. The shoulder surfing resistant system is used for this purpose. For DOS attack, a software puzzle will be generated randomly. The authorized users will get an OTP on their registered mobile number. And also the exact correct solution of the puzzle will be sent. The users who are unable to solve the puzzle will be identified as attackers.

1.1 Software Requirements

1) Operating System: Windows family
2) IDE: Netbeans

3) Web Technologies: Html, Html-5, JavaScript, CSS, JSP
4) Web Server: Tomcat 7/8
5) Programming Language: Java (1.7/1.8)
6) Database: My SQL5.5

1.2 Hardware Requirement

1) Hard disk: 100 GB
2) RAM : 1 GB

1.3 Problem statement

To develop a shoulder surfing resistant authentication system and automatic software puzzle generator using PassMatrix and puzzle core generation algorithm to detect and prevent the DOS and shoulder surfing attack.

2. SYSTEM ARCHITECTURE

In our system firstly the user logins to his account using graphical password. After successfully login, user uploads file on the server. The server encrypts that file using AES algorithm. Then user shares file with another user, by selecting the particular user and then sends the file. After receiving file from user receiver clicks on that file for downloading, but for this he first has to solve the puzzle. This software puzzle is generated by server and it sends a hint of the puzzle and an OTP only to registered valid receivers on their mobile number. With the help of that hint, receiver solves the puzzle and then enters OTP. Answer of the puzzle is send to the server and it checks whether the answer of the puzzle and OTP is correct or not. If both are correct then receiver can successfully download the file, but if receiver is not able to solve the puzzle for three times then the admin detect the receiver as attacker and detects the attack. Finally admin classifies between attacker and valid user. Admin prevents attack by blocking the IP address of attacker for sometime.

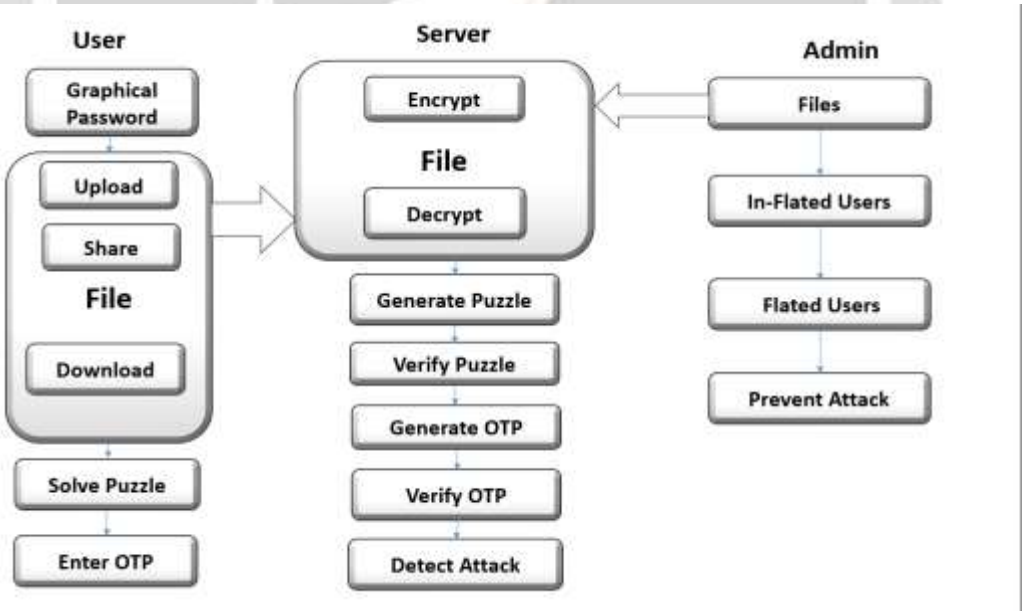

Fig -1: System Architecture

3. MATHEMATICAL MODEL

The DFA has five tuples : (Q, ∑,δ,q0,F)

- Q is a finite set of states,
- ∑ is a finite set of input symbols called the alphabet.
- δ is a transition function.
- q0 is initial state,
- F is Final state
- Q=s1,s2,s3,s4,s5, is a set of states
- ∑ =I0,I1,I2,...,In, is the set of users files
- q0=s1, is the initial state
- F=s6 is the final state
- s1=Users must be registered
- δ(s1, Graphical password login)=s1
- δ(s2,Upload file)=s2
- δ(s3,Send file)=s3
- δ(s4,Puzzle generation)=s4
- δ(s5,OTP generation)=s5
- δ(s6,Puzzle solving)=s6
- δ(s7,Download file)=s8
  Success Conditions: Solve the puzzle
  Failure Conditions: Unable to solve the puzzle.

4. ALGORITHMS TO BE USED

Random Number Generation: This algorithm is used to generate the OTP.
Input: 64 character a to z=26, A to Z=26, 0 to 9=10, and " \. /"=2
Steps:

1. To generate the matrix with row and column 8*8.
2. Put 0 to 63 numbers into matrix.
3. Select one random number from 0 to 63.
4. For putting number into matrix system check number is already present or not.
5. If number present then perform Step3. If not present then put into a matrix and go to step 3.
6. Do step 5 repeatedly up to 0 to 63 inserted into matrix.
7. Print The Matrix.
8. Now Get string which have 64 character " a to z=26, A to Z=26, 0 to 9=10, and. /=2".
9. Get number present into matrix sequentially [0][0] to [8][8] i.e., total 64 character .
10. Select index of string from 64 char. put into that current location.
11. Do step 9 and 10 repeatedly up to [8][8] number.
12. Print Current Matrix With String Char.
13. Display a matrix With Random Printing
14. Stop

AES Algorithm: The AES algorithm is used to encrypt and decrypt files which we are going to upload.
Steps:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

Puzzle Generation: In order to construct a software puzzle, the server has to execute the module:

1. Select 4 random numbers and assign it to A, B, C, D, and select random 3 operators from +, -, *, /.

2. Generate the puzzle and display it on user screen.
3. Send answer to user through email.

4.1 Advantages

1. Graphical password scheme is secure and efficient.
2. Stalkers won't be able to know the password by shoulder surfing resistant system.
3. Complex password scheme with easy user interface.
4. Helps users to login in their account more securely.
5. Private files will be secured

4.2 Disadvantage

1. Time consuming from the users point of view.

5. CONCLUSION

The Identifying an attacker in a network is a difficult task. To reduce the possibility of user's account from getting hacked, we have used the shoulder surfing resistant system based on graphical passwords using PassMatrix technique. In DOS attack, the server is unable to fulfill the requests of the clients if it is overloaded due to traffic. Our proposed software puzzle solving scheme is a computationally expensive task. And thus, by keeping the clients busy, the server will get time to fulfill every request. In addition, the attacker among the clients will also be identified. The registered authorized users will get the exact solution of the puzzle, so they will be able to solve it in the given time. And the users who are unable to solve or solving it in some other way will be considered as attacker.

6. ACKNOWLEDGEMENT

It gives us immense pleasure to thank our project guide Prof. Khushal Khairnar for his valuable suggestions and guidance throughout course of study and timely help in completion of our preliminary project work on "Automatic software puzzle generator and shoulder surfing resistant system to detect and prevent attacks." We would also like to thank our project coordinator Prof. Subhash Rathod and all other faculty members of Computer Engineering department who directly or indirectly kept the enthusiasm and momentum required to keep the work done. We also thank everyone who have coordinated and helped us throughout the work.

7. REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE, 2016, Volume: PP,pp: 1 - 1.

[2] YongdongWu, Zhigang Zhao, Feng Bao and Robert H. Deng, "Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service", IEEE, Volume: 10 ,Jan. 2015, pp: 168 – 177

[3] Yves Igor Jerschow, Martin Mauve , "Non-Parallelizable and Non-Interactive Client Puzzles from Modular Square Roots", Science direct Access, Volume 35, June 2013, Pages 2536

[4] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", research.ijcaonline, Volume 67 No.19, April 2013, pp.0975 8887

[5] Jeff Green, Joshua Juen, Omid Fatemieh, Ravinder Shankesi, Dong Jin, Carl A. Gunter, "Reconstructing Hash Reversal based Proof of Work Schemes", ACM Access , 29 march 2011 , pp.10-10

[6] Ari Juels, John Brainard , "Client Puzzle: A cryptographic counter- measure against depletion attack", researchgate, January 1999