SESSION PASSWORDS USING THREE LEVEL AUTHENTICATION SYSTEM

Ashwini Deshpande[1],Suchita Singh[2], Amrita Kharga[3],Dr.Lata Ragha[4]
Computer Department, Terna Engineering College,University of Mumbai
deshpandeashwini171@gmail.com
singhsuchita96@gmail.com
amrita2192@gmail.com
lata.ragha@gmail.com

***Abstract*—** Today, there are many authentication schemes used in the accessing the private and extremely sensitive data. However these methods have many loopholes by which data can be extracted and used by unauthorized person. Authentication by traditional methods like textual or graphical password may suffer from many attacks. Generally user select password that is easy to remember.

The new System is required that aimed to achieve the highest security in authenticating users. We propose an authentication methodology that involves three levels of user authentication which includes textual password, Image Authentication and Color Authentication. This system is vulnerable to various attacks and is even user friendly. It includes session login which will provide a high level of security to the user. As there are three levels the drawbacks of one level gets overcome by the another level and overall system performance is increased. Three Level Authentication systems will help the user to protect his data secure from the unauthorized user..

Index terms- **Authentication, Security, Three Levels, Image, Color,**

I. INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what it's packaging and labeling claims to be .If the sender and receiver of information cannot properly authenticate each other, there is no trust in the activities or information provided by either party. Authentication can involve highly complex and secure methods or can be very simple.[1] The most common methods used for authentication is textual password, random and lengthy password make the system secure but main problem is the difficulty of remembering these passwords.

Three Level Authentication System is a multifactor authentication scheme. It is designed to combine the benefits of the existing system with the newly proposed methods and removing the threats of the existing system. It uses session passwords for increasing the security.

Three Levels are as follows:

- Security at level 1 has been imposed by using Text based password (with special characters), which is a usual and now a traditional method.
- At level 2 the security has been imposed using Image Authentication where the user will be asked to arrange cropped Images.
- After the successful clearance of the above two levels, the Level 3 Security System will then generate a one-time password that would be valid for only one login session.

II. VULNERABILITY OF AUTHENTICATION SYSTEM

A. *Dictionary Attack*

A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document [2].

B. Brute Force Attack

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.[2]

C. *Shoulder Surfing Attack*

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone.[1]

D. Eaves Dropping

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. The term *eavesdrop* derives from the practice of actually standing under the eaves of a house, listening to conversations inside.[3]

E. Guessing

Guessing can't be a threat to the pair based because it is hard to guess secret pass. Here a legitimate users access rights to a computer and network resources are compromised by identifying the user id/password combination of the legitimate user [4]

III. THREE LEVEL SCHEME

The **First level** will be the Textual Password**.** Textual Password based Authentication is the most widely used method to verify the validity of a user. User has to enter an ID and provide their password to begin using a system. User authentication authorizes human-to-machine interactions in operating systems

Registration Phase

If a user wants to register with a server, he chooses a password

Step 1: User submits ID and Password to server through secure channel

Step 2: If the user is a new user then he will fill up the form and give all his details to the system.

Step 3: Server will check either password is correct or not, if not then display incorrect password.

Step 4: If password is correct then show successfully login and direct to second level. Step 5: If password is incorrect then security questions will be asked to the user or new password will be send on his email.

The first level suffers from Guessing, Shoulder surfing, Dictionary Attack, Brute- Force Attack.

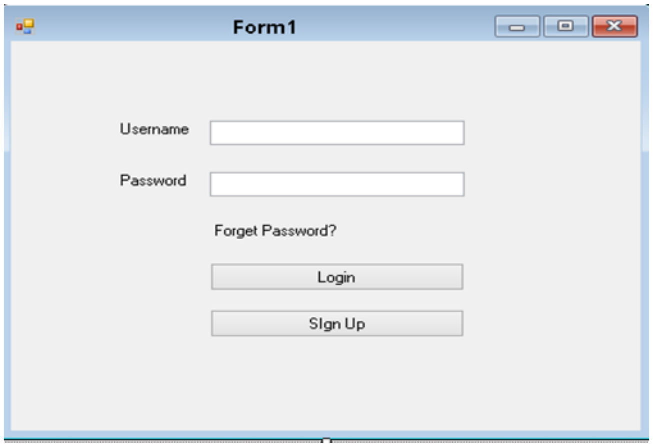


Figure1. Initial Login in the System

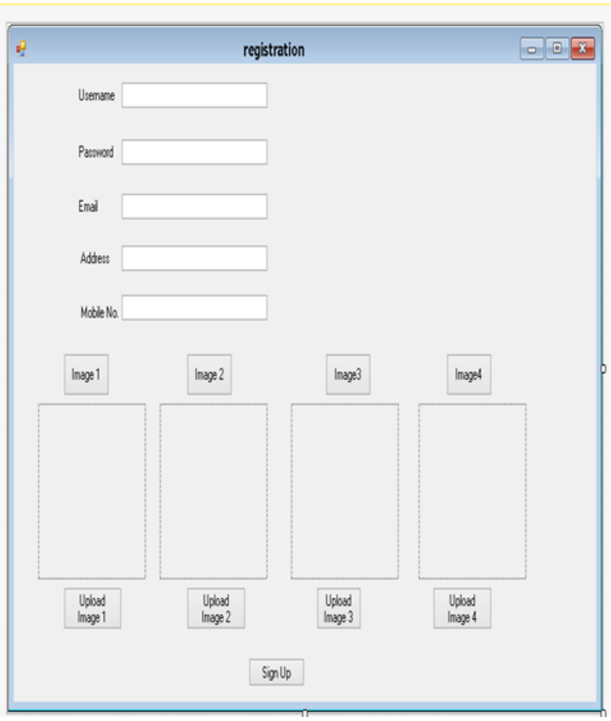


Figure2. Registration Form for new user

The **Second level** will be the Image password. User has to select five images at the time of registration. And at the time of Login the one of the selected image will be displayed in cropped and randomly arranged matrix format. User has to arrange those cropped image in correct order for authentication. And for every session the image will be displayed from registered images.

In second level,

Step 1: User submits image by rearranging cropped image

Step 2: Server will check either image is correct or not, if not then display incorrect image.

Step 3: If password is correct then show successfully login.

Step 4: If user is clicking forget password then other image will come from the registered images.

Image Authentication will overcome from the attacks like shoulder- surfing and eavesdropping. For every session a new image will get displayed so, Theses attacks will not take place.

However, this step can still suffer from the attacks like guessing, dictionary attack, Brute- Force Attack.

The **Third Level** process is much preferable and secured than other two levels. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

Step 1: User will get a color strip and matrix as input.

Step 2: The user will enter the password by remembering the color codes and using the given inputs.

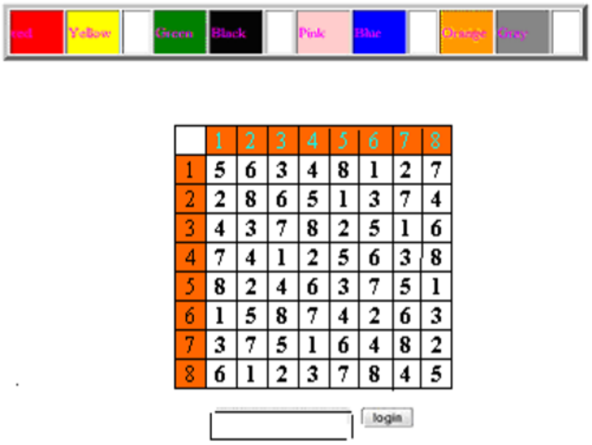
Step 3: If password is correct then show successfully login.

Step 4: If wrong password then logout of the session

Color Authentication will overcome from All the Attacks like Brute-Force, Eaves

Dropping, guessing. The randomly generated

Matrix and session gives it extra security.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Figure3.Color Authentication Login

Three Level Authentication System can be applied in following areas:

1. Army Security
2. Education System
3. Banking Sectors
4. Corporate World

IV. MECHANISM LEVELS

The mechanism shown above will display the flow of the system from the beginning.

First, the system will check whether the user is registered or not. If not, then user will register himself by giving login-id and password and will give all the details like chosen images and color codes. All the details will be saved in the database.

First level consists of traditional login. The user will authenticate him by entering the correct user-id and password. Then, He will be directed to second Level and the session

will begin after successfully arranging the puzzled images the color authentication will get begin this will has matrix and color codes which will help in Authentication. After the successful login of the above step user will be logged in. However, if at any step the users fails to authenticate himself, the session will get expire and user again has to start from the beginning.

V. CONCLUSION

In Three level authentication System Textual password and Image password is easy to remember and it is overcoming the various attacks and is also easy for user to access. Third level generates session passwords and is resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. We have also use the Encryption standard like AES standard.

As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs. It prevents from the following attacks:

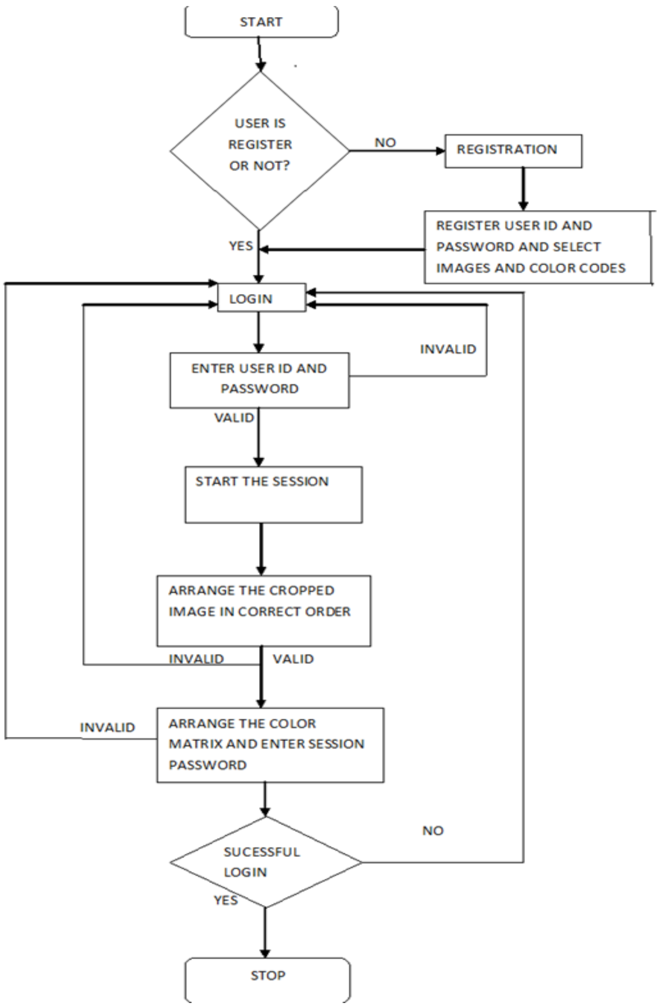

START
USER IS REGISTER OR NOT?
NO
REGISTRATION
REGISTER USER ID AND PASSWORD AND SELECT IMAGES AND COLOR CODES
YES
LOGIN
INVALID
ENTER USER ID AND PASSWORD
VALID
START THE SESSION
ARRANGE THE CROPPED IMAGE IN CORRECT ORDER
INVALID
VALID
INVALID
ARRANGE THE COLOR MATRIX AND ENTER SESSION PASSWORD
NO
SUCESSFUL LOGIN
YES
STOP

Figure4.Flowchart of the System

Dictionary Attack: These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

Shoulder Surfing: These techniques are Shoulder Surfing Resistant. In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains hidden so the session password can't be enough to find secret pass in one session..

Guessing: Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 36 4. The hybrid textual scheme is dependent on user selection of the colors and the ratings. If the general order is followed for the colors by the user, then there is a possibility of breaking the system.

References

. N.S.Joshi "Session Passwords using grides and colors for web application and PDA". In International Journal of Emerging Technology and Advanced Engineering,volume 3,Issue 5, May 2013.

2. M Sreelatha,M Shashi, M Anirudh "Authentication Schemes for Session Passwords Using Color and Images". In International Journal of Network Security and it's applications,Vol 3, No.3,May 2011.

3. Techtarget,site:http://searchfinancialsecurity.techtarget.com/definition.

4. Omnisecu.com,site:http://www.omnisecu.com/security/password-guessing-attacks.php

5. Authentication schemes for session password using color and special characters by Rohit Jagtap,Vaibhav Ahirrao, Vinayak Kadam, Nilesh Aher.