International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 8 5220 - 5223

Pair Based Authentication using Dynamic Grid

Janhavi Thakur
M.E.Scholar,
Department of Computer Engineering,
TCET, Mumbai, India

Sheetal Rathi
Assistant Professor
Department of Computer Engineering,
TCET, Mumbai, India

Abstract:- Authentication is an important step in Login to the system. In this paper we are implementing one scheme for Mobile Social Network which makes the authentication process secure compare to the other schemes. Many schemes were proposed to secure the system. We first explore some major schemes proposed for the Authentication process. Due to the lots of attacks in the cyber world, high performance and secure login schemes are becoming important and we are implementing one such scheme in our implementation of mobile social network: Pair based authentication.

General Terms:
Authentication, Security
Keywords:
Mobile Social Network, Session Passwords, Pair Based Authentication Dynamic Grid.

*****

1. Introduction:

Social networking has become an important factor in our life, which allows us to connect with the families and friends. Now a day mobile are playing an important role in day to day life. They have come up with the tag line anywhere; anytime that has given rise to the term Mobile Social Network.

The use of mobile social networks is increasing day by day. More and more people are registering to avail the services. The user's personal data is very sensitive information. So the networking sites should guarantee the users that there data will be safe. Here comes the question of the security to the system.

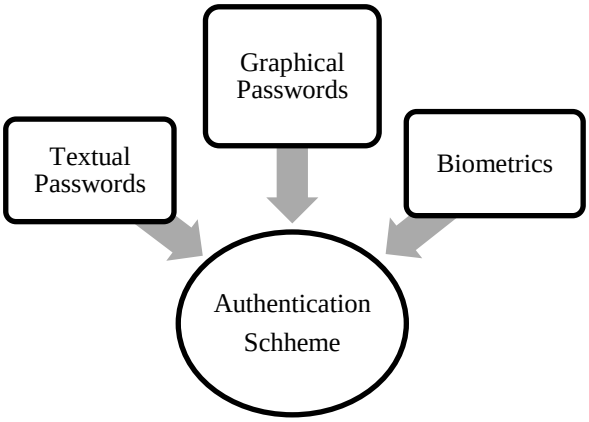
Authentication is the main step to access any social website, where user have to put username and password i.e. some credential to the system so that the they will understand genuine user is accessing the website. Many schemes and techniques are available to provide the authentication.

In this paper we have first listed out all the authentication schemes. We have focused on text passwords, graphical passwords and biometrics. The possible attacks on them were shortlisted. Then we have implemented Pair Based Dynamic Grid Authentication scheme and compared its parameters with the existing schemes.

2. Related Work:

We have divided the term Security in two processes Authentication, Authorization. Several techniques are present in each area.

In Authentication phase, the user has to submit correct credentials which are already stored in the system. After that user is been given the access to the system. There are various ways of authentication techniques i.e. textual passwords, Graphical passwords and Biometrics



.

Fig.1 Authentication Scheme

Among the various authentication techniques textual password is popular. It consists of the string of alphabets and special characters. Generally the users have tendency to choose simple passwords i.e. Spouse's name, maiden name, building name etc. User can choose any arbitrary or lengthy password to avoid such attacks. But studies have found that they are not easy to remember.

There are various attacks possible on the textual passwords like Brute Force attack, Eavesdropping, Dictionary attack, Social Engineering, Key Logging and Shoulder Surfing etc [1, 2, 3].

Graphical passwords were introduced to overcome the attacks faced by textual passwords mostly shoulder surfing, key logging etc. Various graphical password schemes were introduced by many authors [4, 5, 6].

In such a scheme the user have to enter the username. After that the graphical objects will be displayed on the screen. Depending on the scheme either user have to place images from random to correct order which were preselected by user while registration.

Using mouse, touch pad, touch screen user has to select the objects. Also signatures can be used for authentication. But even if the slight change is found the authentication is stopped.

Though the system is secured compare to the textual passwords it has lots of disadvantages. User verifies or authenticate only when proper sketch is drawn. Extra sensitive key pads are required for such scheme. Also the time required in authentication process is longer.

The biometric scheme is used for authentication which is based on the image recognition process. In this scheme first the image is pre-processed and then matched with the database. Iris recognition, face recognition, thumbs recognition are the various types of biometrics.
It is one of the good authentication schemes as it's real and unique. Also it doesn't have the fear to be stolen. But this scheme is expensive also the process is time consuming [7, 8].

The Pair Based Authentication scheme [9] helps to remove the drawbacks of the above schemes. It helps to avoid various attacks on the login system such as dictionary attack, brute force attack, shoulder surfing attack etc. But Pair Based Authentication Grid is static, due to which key logging attack is possible. So we will implement new authentication scheme Pair Based Dynamic Grid Authentication in which the display changes after every session.

The scheme Pair Based Dynamic Grid Authentication consists of three phases: Registration, Login and Verification Phase. In the Registration phase User registers the password. When login is to be performed users have to enter the credential from the shown grids. The system then verifies the password with the stored database password. As the system is designed to work with pair of characters only even length passwords are allowed.

3. Pair Based Authentication using Dynamic Grid:

The scheme Pair Based Dynamic Grid Authentication helps user to keep the login process secured. It also removes the disadvantages faced by various schemes invented before. Following are the steps which have to be followed so as to enter the password. The user makes the pair of the password. First user checks for the row and then column. Now he/she finds the intersecting character and enters it as password. After successfully entering all the password logins to the system.

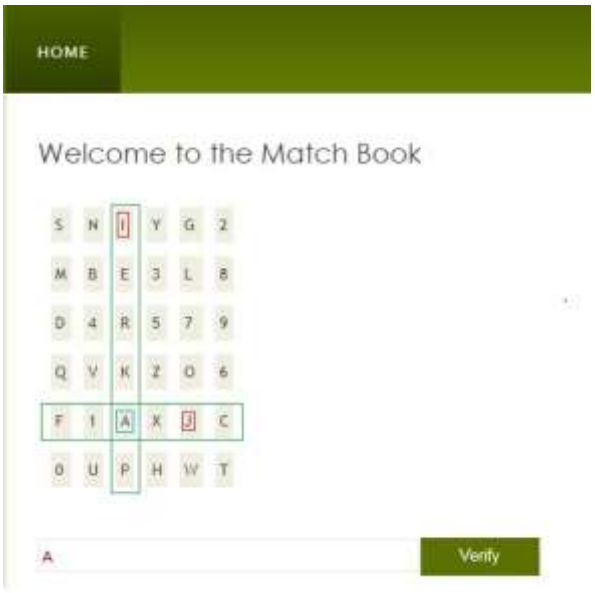


Fig.4 Pair Based Dynamic Grid Authentication Scheme

The below are the steps which are used for the authentication process.

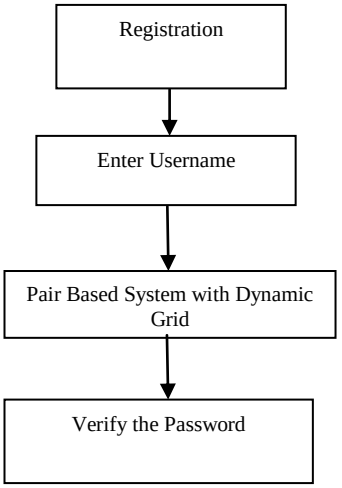


Fig.3 Flow diagram of Pair Based Dynamic Grid

Authentication Scheme

This authentication scheme consists of three steps
Step 1) Register Username and Password
Step 2) Login to the system
Step 3) Verify the stored password

 ISSN: 2321-8169
5220 - 5223

4. Experimental Results:

All the experiments were executed on 2.40 GHz Intel i5 processor with 4GB RAM. The program code is written in C# and executed using .Net framework.

As we can see in the above screenshots of Pair based authentication using dynamic grid scheme, the interface changes after each session, thereby thwarting any key logging attack on the user.

Table 1 shows textual passwords, graphical passwords, biometrics and Pair Based Dynamic Grid Authentication are compared in various parameters. From which it is clear that Pair Based Dynamic Grid Authentication requires low cost, it gives high protection level, processing time is also low and it doesn't require
additional hardware. We can see that it is the best technique.

Table 1. Comparison of Authentication technique

Authentication Schemes	Cost	Protection Level	Processing Time	Additional Hardware Required
1)Textual Password	Low	Medium	Low	No
2)Graphical Password	High	Medium	High	Yes
3)Biometric	High	High	High	Yes
4)Pair Based Dynamic Grid	low	High	Low	No

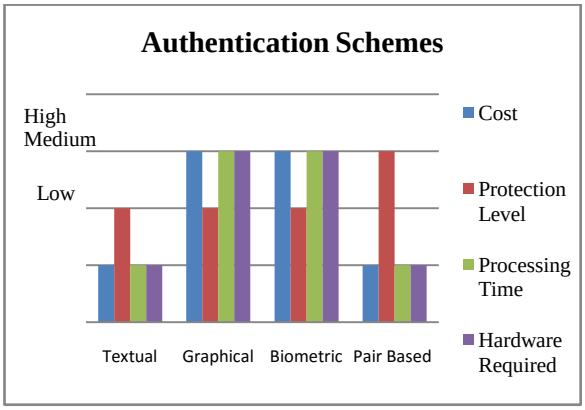


Fig.5 Comparison of Paired Based Authentication with other schemes

Table 2 enlists the attacks possible on the above scheme.
We can see from the table that except textual password all other schemes, too resist various attacks but their implementation cost is high. Again we can say that Pair Based Authentication using Dynamic grid is the best technique.

Table 2.Attacks on the Authentication technique

Authentication Schemes	Attacks	Resistant to Attacks	Cost
1)Textual Password	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping, Guessing	--	Low
2)Graphical Password	--	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping	High
3)Biometric	--	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping	High
4)Pair Based Dynamic Grid	--	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping	Low

5. CONCLUSION:

Conventional authentication schemes like Textual Password and others have experienced limitations while handling the login process. Though textual passwords are the simplest way to handle the login process it is more prone to attacks. Other schemes graphical password requires more processing time than the textual passwords hence lessen the performance. Also it provides medium security. Another traditional scheme, biometrics faces the challenge for maintaining the high precision equipments required for scanning iris, thumbprint, etc. Also the processing time is more compared to the other schemes. It takes significant amount of time whenever the matching is to be performed

between the users entered data and database data. Implemented authentication scheme comes over these three disadvantages.

Experimental results of Pair Based Dynamic Grid Authentication show that it is efficient in reducing processing time by taking texts as the input. Also, shows the cost for designing the system is very less as no external hardware is required for the authentication process. It is resistant to many attacks and provides high protection level. The implemented authentication scheme is faster and more secured compared to the other schemes in the market. More websites should adopt these schemes to avail the advantages given by it.

6. ACKNOWLEDMENT:

We are greatly indebted to **Dr.R.R.Sedamkar** for his guidance and enlightened comments, which has helped in completing work successfully.

REFERENCES:

[1] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password cracking using probabilistic context-free grammars,” in Proc. IEEE Symposium on Security and Privacy, 2009.

[2] Fujita, K. and Y. Hirakawa, “A study of password authentication method against observing wrapper approach for feature subset selection in Attacks”, 6th International Symposium on Intelligent keystroke dynamics identity verification, Systems and Informatics, SISY 2008.

[3] D. Florencio and C. Herley, “A large-scale study of web password habits,” in Proc. WWW’07, 2007.

[4] Eljetlawi, A.M.; Fac. of Eng., Univ. of Tajoura, Tripoli, Libya," Graphical password: Existing recognition base graphical password usability", IEEE, March 2010

[5] Almulhem, A.; Comput. Eng. Dept., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia,"A graphical password authentication system", IEEE, FEB 2011

[6] XiaoyuanSuo,; Ying Zhu; Owen, G.S, "Graphical passwords: a survey", IEEE, DEC 2005.

[7] Ahmed, A.A.E. and I. Traore, “Anomaly Intrusion Detection Based on Biometrics, IEEE Proceedings, IAW '05.

[8] Varun Kacholia and Shashank Pandit,”Biometric Authentication Using Random Distribution”, Canadian IT Security Symposium (CITSS), 2003

[9] VAISHNAVI PANCHAL*, CHANDAN P. PATIL,“Authentication Schemes for Session Password**”,** IJSER 2013

[10] Shakir, M. and Abdul Ayaz Khan,”S3TFPAS Scalable shoulder surfing resistant Textual-Formula base Password Authentication system” IEEE, 2010