ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

Two-Factor Authentication using Mobile Phone

Vinit Patel, Jay Shah, Saumya Lahera

B.E. Student, Dept. of Computer Engineering, MCT's RGIT, Mumbai, India

B.E. Student, Dept. of Electronics, KJSIEIT, Mumbai, India

B.E. Student, Dept. of Computer Engineering, SAKEC, Mumbai, India

ABSTRACT: Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eaves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this project, a technique is proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

KEYWORDS: Session , Passwords ,Shoulder Surfing.

I INTRODUCTION AND MOTIVATION

The most common method used for authentication is textual password. The vulnerabilities of this method like eaves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked.

The alternative techniques are graphical passwords and biometrics**,** but these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow.

There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices.

The two new authentication schemes are proposed for PDAs. These schemes authenticate the user by session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords.

II PROBLEM STATEMENT

Following are the problem that occurs in previous method use for the password schema. Generally various attacks that is affected in the textual password. and the attacks are:

2.1 DICTIONARY ATTACK

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

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.In our project The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

2.2 SHOULDER SURFING

These techniques are Shoulder Surfing Rsistant.

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.In hybrid textual scheme, the randomized colors hide the password.In this scheme, the ratings decide the session password. To overcome this session password you can't find the ratings of colors.

2.3 GUESSING

Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 364.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.

2.4 BRUTE FORCE ATTACK

These techniques are particularly resistant to brute force due to use of the session passwords.
The use of these will take out the traditional brute force attack out of the possibility.

III PROPOSED SYSTEM

3.1 WORKING OF THE PROPOSED SYSTEM

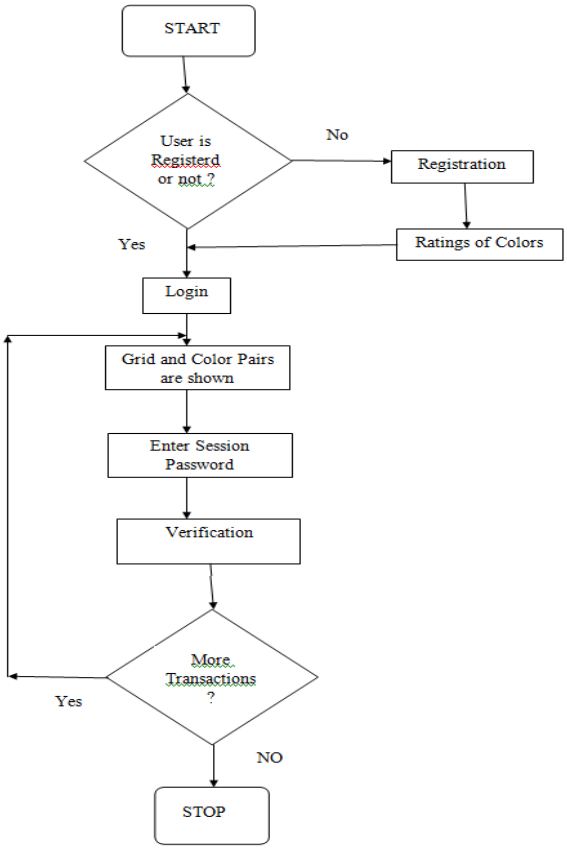

Fig 3.1 Work Flow

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

3.2 DATA FLOW DIAGRAM

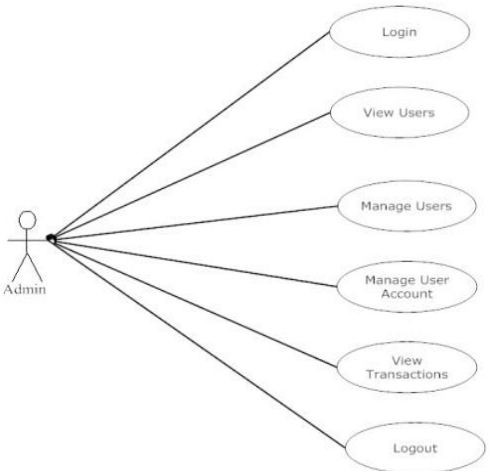

Fig 3.2 Admin Use Case

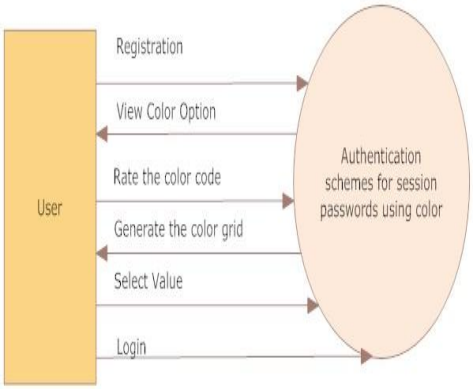

Fig 3.3 DFD Context Level

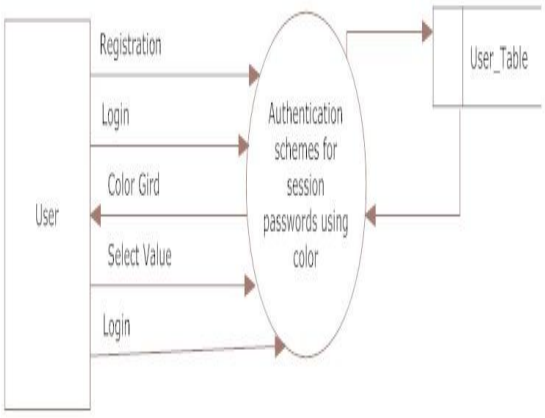

Fig 3.4 DFD First Level

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

IV IMPLEMENTATION DETAILS

4.1 RATING COLOR HYBRID PASSWORD ALGORITHMS

In our project we are using "Rating Color Password Algorithm". It is novel approaches to in the domain of password and security. The steps of above algorithm are follows, for the simplicity we divided the algorithm in two parts, one part is registration process and second part is login process.

4.1.1 Algorithm 1: Registration Process

Step 1: During registration process, the system displays the one-dimensional color grid.

Step 2: The user gives the rate from 1 to 8. The color in color grid is static that mean the color order is not change for every users. The color order is as follows, RYGBPBOG (R=Red, Y=Yellow, G=Green, B=Black, P=Pink, B=Blue, O=Orange, V=Violet). Also same rating can be given to the different color.

4.1.2 Algorithms 2: Login Process

Step 1: When user enters the username the system display the interface based on color selected by the user. The login interface consists of grid of size 8*8 along with the color grid.

Step 2: The user selects the session password based on color rating. This time color grid is which enclosed 8 color separated 2-2 color into 4 blocks. And user has to select the session password based on that block. The 8*8 grid is look like as,

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

Fig. 4.1 Color Rating

4.1.3 Algorithm 3: How to select the session password form the 8*8 grid.

Step 1: The Color grid is as follows,

R	Y		G	B				P	B		O	G

Block 1 **Block** **Block 3** **Block**

Fig . 4 .2 Color Grid

The color grid is separated in 4-blocks. From that we are selecting the session password.

Step 2: From every block the first color is row and second color is column. And interesting the row and column of every block value is our session password.

4.2 METHOD FOR RANDOM NUMBER GENERATOR

A linear congruential generator (LCG) is an algorithm that yields a sequence of randomized numbers calculated with a linear equation. The method represents one of the oldest and best-known pseudo random number generator algorithms. The theory behind them is easy to understand, and they are easily implemented and fast, especially on computer hardware which can provide modulo arithmetic by storage-bit truncation. The generator is defined by the recurrence relation.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

$$X_{n+1} \equiv (aX_n + c) \pmod{m}$$

Where X is the sequence of pseudorandom values, and

$m,\ 0 < m$ — The "modulus"

$a,\ 0 < a < m$ — The "multiplier"

$c,\ 0 \leq c < m$ — The "increment"

$X_0,\ 0 \leq X_0 < m$ — The "seed" or "start value" are integer constants that specify the generator. If c = 0, the generator is often called a multiplicative congruential generator (MCG), or Lehmer RNG. If c ≠ 0, the method is called a mixed congruential generator.

Fig. 4.3 Admin Database

Fig. 4.4 User Registration

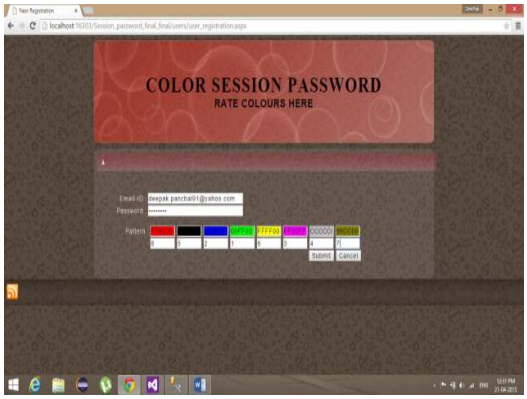

Fig. 4.5 Color Rating & Password Generation

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

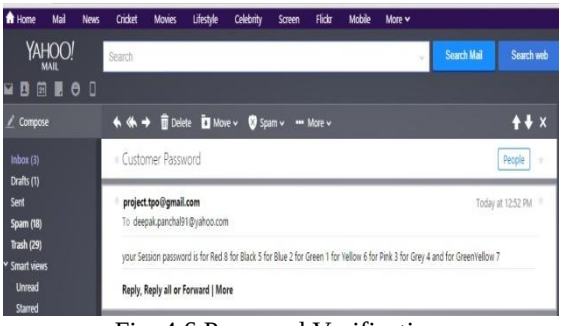

Fig. 4.6 Password Verification

Fig. 4.7 Session Password Generation

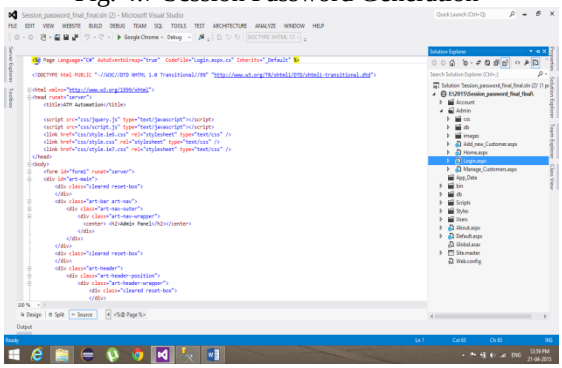

Fig. 4.8 Code.

V.TECHNOLOGIES USED

5.1 HARDWARE REQUIREMENTS

System : Pentium IV 2.4 GHz.
Hard Disk : 40 GB.
Ram : 512 Mb.

5.2 SOFTWARE REQUIREMENTS

Operating System : Windows 7.
Coding Language : ASP.Net with C#
Data Base : SQL Server 2008.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

5.3 ASP.NET

Active Server Pages (ASP) is a unified Web development platform that provides the services necessary for developers to build enterprise-class Web applications.

5.4 MICROSOFT SQL SERVER 2008

Business today demands a different kind of data management solution. Performance scalability, and reliability are essential, but businesses now expect more from their key IT investment.

SQL Server 2008 exceeds dependability requirements and provides innovative capabilities that increase employee effectiveness, integrate heterogeneous IT ecosystems, and maximize capital and operating budgets.

1 Easy-to-use Business Intelligence (BI) Tools

.2 Self-Tuning and Management Capabilities

3 Data Management Application and Services:

VI.CONCLUSION AND FUTURE WORK

These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. This technique use grid for session passwords generation. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensive. The proposed system prevents users from choosing weak passwords .In this the technique is proposed to generate session password using text and colors which are resistant to shoulder-surfing .This method is used in Personal Digital Assistants.

The proposed system can be used widely in banking application for security purposes. ATM machines where security should be very high.

REFERENCES

[1] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[2] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[3] W. Jansen, "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium, 2003
[4] D.L. Crook, "Evolution of VLSI reliability engineering," in Proc. Int. Rel. Physics Symp., pp. 2-11, 1990.
[5] Biometrics Authentication Techniques for Intrusion Detection System Using Fingerprint Recognition (IJCSEIT).
[6] Passlogix, site http://www.passlogix.com.
[7] Real User Corporation: Passfaces. www.passfaces.com