Proposed 4-D Authentication Mechanism

Ms. Shraddha Gajare.
M. E Student,
Department of Computer Engineering,
Yadavrao Tasgaokar Institute of Engineering and Technology
gajare.shraddha3@gmail.com

Prof. Vaishali Londhe.
M. E ,
Department of Computer Engineering,
Yadavrao Tasgaokar Institute of Engineering and Technology.

Prof. Nilima Nikam
M. E,
Department of Computer Engineering,
Yadavrao Tasgaokar Institute of Engineering and Technology.

Abstract- Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. Here, we propose 4-D Password scheme to make the existing scheme even more robust and powerful. We propose to different authentication scheme to one system, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in. We proposed a system with graphical password scheme, Color code authentication, OTP based authentication, and Time Elapse Authentication scheme composed as a 4-D Authentication system.

*****

I. INTRODUCTION

Today, in spite of the fact that the secret word confirmation is utilized generally, since clients compose their watchword specifically on screen and tend to make their secret word simple to recollect that, they might be powerless against a few assaults, for example, animal power, speculating, replay, and shoulder surfing. Albeit numerous validation plans were proposed to enhance the ease of use and security, they are still helpless against the shoulder surfing assault. In this anticipate, we propose a 4-D design based confirmation plan which is secure against this assault. Likewise, we dissect the ease of use, wretchedness, and security of the proposed verification plan, contrasted with the other validation plans. Concocting a client validation plan in view of a few recognizable proof plans that is both secure and for all intents and purposes usable is a testing issue. The best trouble lies with the weakness of the passage procedure to coordinate observational assaults, for example, human shoulder-surfing and camera-based recording. This anticipate begins with an examination of a past endeavor at taking care of the passage issue, which depended on a few validation plans like Authentication utilizing a Rotating wheel with 8 divisions, Color Code Authentication, OTP Authentication and Time Elapse Authentication plans. Despite the fact that the strategy required uncomfortably numerous client inputs, it had the value of being straightforward and use. Our investigation that takes both the test and hypothetical methodologies uncovers various genuine deficiencies of the past strategy, including round excess, unequal key presses, exceedingly visit framework blunders, and inadequate flexibility to recording assaults. The lessons learned through our examination are then used to enhance the verification plan. The new plan has the amazing property of opposing camera-based recording assaults over a boundless number of confirmation sessions without releasing any passwords.

II. RELATED WORK

Literature Survey shows existing anti-shoulder surfing mechanism is usually applicable for graphical password scheme for common security applications only, hence there is a need to increase the complexity of This is why, in this paper, we are trying to improve the security of graphical password for mobile devices, by proposing an anti-shoulder surfing mechanism called 4D Graphical Password Authentication.

III. PROPOSED SYSTEM

We propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.

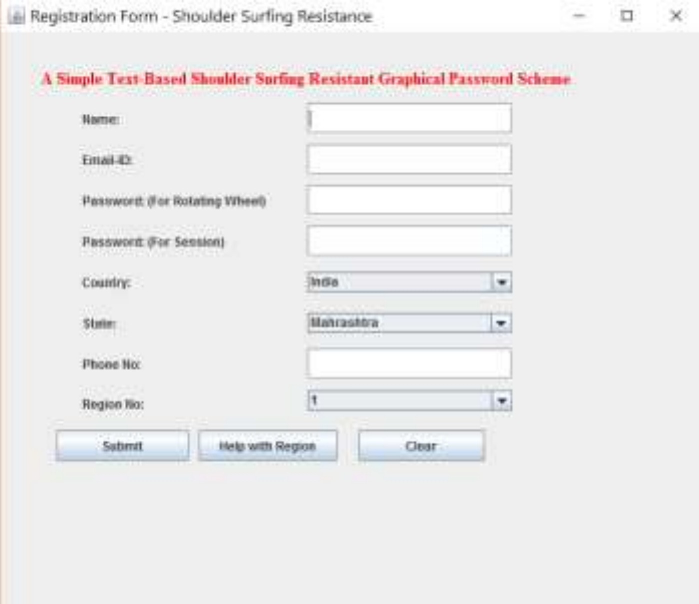
We have divided our proposed work in 4 phases which are as under:

Phase 1: Registration

In Registration, we need to do registration for two authentication schemes,i.e Graphical Wheel and color code registration.

a. Graphical Wheel registration:

The user has to set his textual password K of length L (8≤L≤15) characters, and choose one region from 8 regions assigned by the system. The remaining 7 regions not chosen by the user are his decoyregions. And, the user has to register an e-mail address for re-enabling his disabled account. The registration phase should proceed in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS [16][17] or any other secure transmission mechanism. The system stores the user's textual password in the user's entry in the password table.



Registration Form - Shoulder Surfing Resistance

A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme

Name:
Email-ID:
Password (For Rotating Wheel)
Password (For Session)
Country: India
State: Mahrashtra
Phone No:
Region No: 1

Figure 1. Graphical Wheel Registration

b. Color Code Registration:

During registration, user should rate colors as shown in figure 2. The User should rate colors from 1 to 8 and he can remember it as "YRGBOIMP". Same rating can be given to different colors.

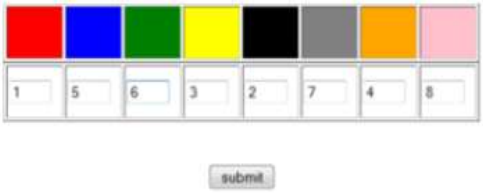


Figure 2: Color Code Authentication

Phase 2: Login Phase

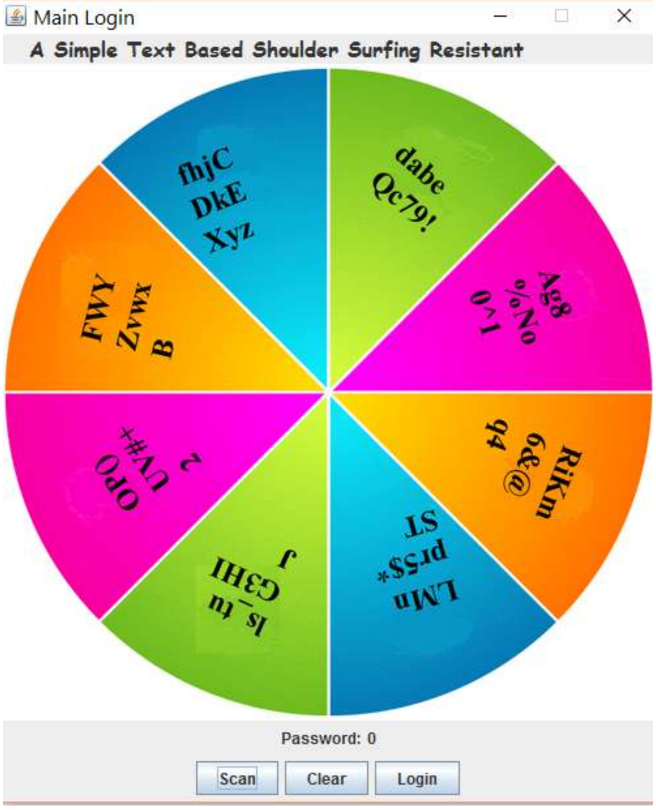
a. For Graphical Wheel

To login the system, the user has to finish the following steps:

Step 1: The user requests to login the system.

Step 2: The system displays a circle composed of 8 equally sized sectors, and places 64 characters among the 8 sectors averagely and randomly so that each sector contains 8 characters. The 64 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." and "/" are in regular typeface, and the 10 decimal digits are in italic typeface. The "Scan" button, and the "Login" button are also displayed on the login screen. All the displayed characters is rotated along the adjacent sector clockwise. Let i = 1. The rotation wheel can be illustrated by an example shown in Fig. 2.

Step 3: The user has to select a charactor in selected sector containing i-th pass-character of his password K, denoted by K_i, into his selected sector, and then clicks the "Scan" button. Let i = i + 1.



Main Login

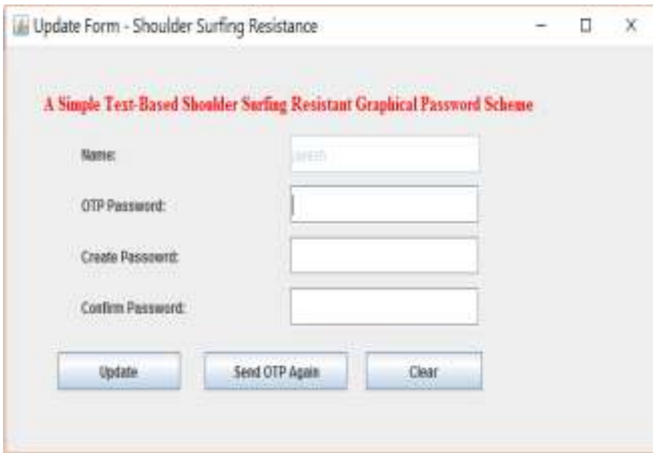
A Simple Text Based Shoulder Surfing Resistant

Password: 0

Figure 3 : Login phase of Rotating Wheel

b. OTP input:

OTP is used when user passed the above scheme and OTP should be Verified to Navigate to next authentication scheme.



Update Form - Shoulder Surfing Resistance

A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme

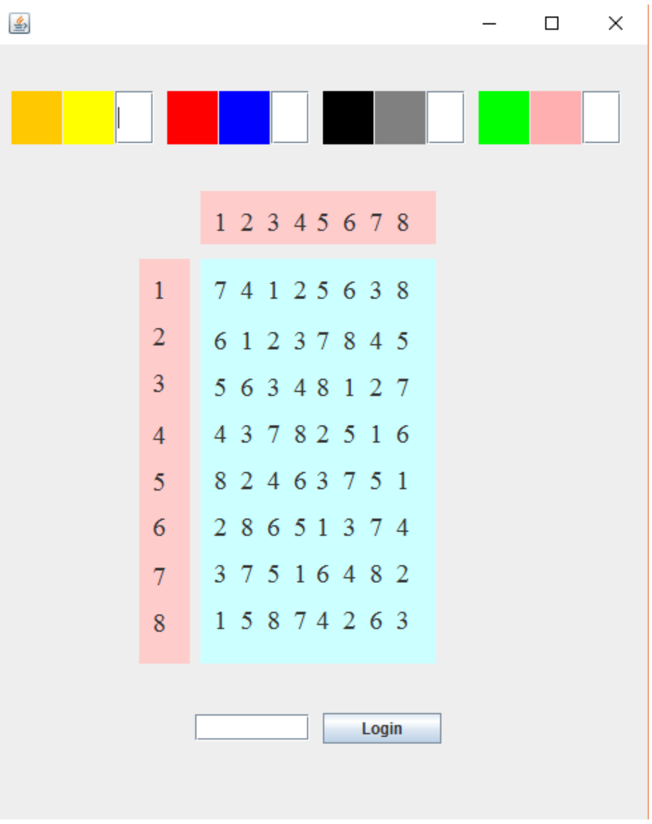
Name:
OTP Password:
Create Password:
Confirm Password:

Figure 4: OTP

c. Color Code Authentication

Once the OTP is validated, User is navigated to color code scheme.

During the login phase, the login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid. Figure shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password.



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

Figure 5: Color Code login

Consider the figure 2 ratings and figure 5 login interface for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e. the same method is followed for other pairs of colors. For figure (6) the password is “3573”. Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

d. Average Time:

Average Time of a user to complete all Authentication phases is recorded and it is compared with a tolerance value which is relatively small. User gets authenticated only after passing this last phase.

IV. ALGORITHM:

1. Start Timer and Store Starting Timestamp, let Staring Time (ST) = current Time.
2. The user requests to login the system.
3. The system displays a circle composed of 8 equally sized sectors, and places 73 characters among the 8 sectors averagely and randomly so that each sector contains up to 10 characters. The 73 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the others symbols are in regular typeface, and the 10 decimal digits are in italic typeface. The “Confirm” button, and the “Login” button are also displayed on the login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise.
4. The user has to rotate the sector containing the i-th pass-character of his password K, denoted by K_i, into his pass-color sector, and then clicks the “Confirm” button. Let i = i + 1.
5. If i < L, the system randomly permutes all the 73 displayed characters, and then GOTOs Step 3. Otherwise, the user has to click the “Login” button.
6. If entered Password is Correct then to user navigates on next login phase.
7. Else
8. Error Message is displayed to User and Exit Application
9. Random One time Password (OTP) is generated and OPT is Send on Registered Email Address.
10. User have to Enter the Genuine OTP which has been obtained from there Registered Email Address.
11. If OTP is Genuine then User navigates to next Login Phase
12. Else
13. Error Message is displayed to User and Exit Application
14. Next Dimension of Login phase consists of grid of size 8×8.
15. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.
16. The first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. So the first letter of session password is 1st row and 3rd column intersecting element.
17. The same method is followed for other pairs of colors. Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

18. After Entering a Valid Password User is navigated to Next Dimension of Login Phase
19. Else
20. Error Message is displayed to User and Exit Application
21. Record the Current Time and Calculate the stay on user Time for All login phases i.e. Current Time = CT,
22. Let Stay on User time = Starting Time (ST) – Current Time (CT)
23. If Stay on Time is Equal to Average Stay on Time with Tolerance of 15 Seconds then
24. Authenticate User
25. Else
26. Error Message is displayed to User and Exit Application.
27. Home Screen is displayed and New Average Stay on Time is Calculated using (Stay on User Time + Average Stay on Time) / 2.

V. ANALYSIS:

Let's say we have a 12 character password for Phase 1 containing mixed-case alpha characters, numbers and special Symbols i.e. a-z, A-Z, 0-9, and !@#$%^&*().

Phase 2 will have OTP password which will have 6 Character mixed-case alpha characters and numbers i.e. a-z, A-Z, 0-9.

Phase 3 will have 4 Character passwords containing only numbers 0-9.

So keyspace for such a password will be 72^12 + 62^6 + 46^10

19. 408409 * 10^21 + 56.8002 * 10^9 + 42.4207 * 10^15

But hence we have divided this 62 characters and Numbers into 8 Regions so it becomes

24. 26051 * 10^20 + 56.8002 * 10^9 + 42.4207 * 10^15 = 2.42609 * 10^21

Now, let's say we currently compute hashes at a rate of 3.0x10^{9} (three billion) per second on a modern GPU. At this rate, using the same hardware, we could search the entire keyspace in 808697888674 Seconds which are equal to 25643 years.

So to Crack this Password it will take around **<u>25643</u>** Years. But Hardware will not remain same in this 25643 Years. So we will also consider that Transistor counts will double every 2 years and Hash computation speed is directly proportionate to transistor count. Also there is no upper limit on transistor count.

Then According to Moore's law which states that processing power will double every 2 Years.So we can come up with an equation

A(n) = A(n-1) - C * 2 ^ (N-1) and A(0) = size of keyspace, say 72^12.

lets set C = 3.0*10^9 for hashes computed the first year and assume computing power doubles every year.

Plugging this into wolfram alpha yields this function solution for the recurrence relation:

recurrence relation...

f(x) ~= 19.408x10^21 - 3.0x10^9 * 2^x

Solve f(x) = 0 for x:

x = log (19.408x10^21 / 3.0x10^9) where log is log base 2

x ~= 30.81 years

Cracked in 30 years, but that's a lot of silicon, and you would need a method to seamlessly integrate new hardware into the running program without stopping it.

VI. SECURITY ANAYSIS:

1. Keylogger:

In many cases, the attacker installs an invisible software called a keylogger, which is designed to capture all keys typed through the user’s keyboard and output them as a stream in a text file.This way the attacker finds out the user’s password by browsing through the file. But here, since the nature of pass-word is not textual, this attempt will be a total failure.

2. Shoulder Surfing Attack:

An attacker uses a camera to record the user’s 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical pass-words. However, the user’s 3D password may containbiometric data or textual passwords that cannot be seen from behind.

Therefore, we assume that the 3D password should be per-formed in a secure place where a shoulder surfing attack can-not be performed. Also, with the 4-D password, the nuances of the gesture, even if visible to the attacker, may not be emulat-ed successfully, and also the physique will have to match with the user, since the system would compare it with the earlier recording.

VII. CONCLUSION:

We propose 4-D Password plan to make the current plan significantly more hearty and capable. We propose four distinctive validation plans to one framework, and this will loan more strength and make the assaults on client security significantly more hard to succeed in. We proposed a framework with graphical watchword plan, Color code validation, OTP based confirmation, and Time Elapse Authentication plan formed as a 4-D Authentication framework. The plan deals with the structure of halfway recognizable aggressor model. From security perspective the plan is very powerful against some conceivable assaults, for example, shoulder surfing, speculating secret word, side channel assault, and so on. Furthermore, from convenience perspective the plan is easy to understand and sets aside less time for login. Likewise the plan can be utilized by both math and non-math situated individuals.

REFERENCES

[1] Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan 2013.

[2] Nilesh Chakraborty, Samrat Mondal "Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack", Proceeding of the 2014 IEEE Students' Technology Symposium.

[3] L. Sobrado and J. C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[4] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," *Draft*, 2005. (http://clam.rutgers.edu/~birget/grPssw/srgp.pdf) [3] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," *Proc. of Working Conf. on Advanced Visual Interfaces*, May. 2006, pp. 177-184.

[5] M. M. Group, "http://www.internetworldstats.com/stats.htm," June 2012.

[6] C. Herley, P. C. Oorschot, and A. S. Patrick, "Passwords: If were so smart, why are we still using them?," in Financial Cryptography, pp. 230–237, 2009.

[7] www.webeopdia.com/term/s/shoulder−surfing.html (last access Octeber,2013).

[8] A. Paivio, "Mind and its evaluation: A dual coding theoretical approach,"2006.