3D Password with Session Based Technique for Login Security in Smartphone

Bharti Yerne, Prof. Fazeel.A.Z.Qureshi
Computer Science & Engineering, RTMNU University, W.C.E.M, Nagpur, Maharashtra, India

Abstract:- Up till now many shoulder surfing resistant graphical password schemes have been proposed. However, as most of the users are more familiar with textual passwords than the pure graphical passwords scheme therefore the text-based graphical password schemes have been proposed. But none of the existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors because of that the user can easily and efficiently login system. Next, we provide the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.Now we propose a technique that is 3D password with session based technique for login security in smart phone means we are going to use two level authentications that is simple text based shoulder surfing graphical password as a first level. Whenever we are going to login in smart phone there is one circle occur with multiple random color and circle divided into eight sector which contain characters and alphanumerical which we select as a password. And 3D images as a second level in which whenever user going to start a session in smart phone, number of time 3D images will be change but object will be same which is used as a password on 3D images, which provide more security to the user in smart phone.

*****

1. Introduction

The shoulder surfing attack is an attack that can be performed by the attacker to obtain users password by watching over the user's shoulder when user enter his password. In an existing work, we can see the technique provide for authentication is that there is one circle provide which divide into eight sector having numeric and alphanumeric into each individual sector. And each individual sector having different color. Also there are some key provide for rotate sector to choose color and password either clockwise or anticlockwise and then confirm and login. But anyone can guess this level means someone who is very close to the user then he/she must know the favorites color of user and once the attacker know the entering color of user then he/she is very close to attack the password by guessing attack or dictionary attack. And one drawback is also that this technique only provide for desktop user. As conventional password schemes are vulnerable to shoulder surfing.

In one an existing proposed technique is that there are three shoulder surfing resistant graphical password schemes are provided, first the Movable Frame scheme, second the Intersection scheme and the last one Triangle scheme. However, the Movable Frame scheme and the Intersection scheme have been failure rate. In the Triangle scheme, the user has to choose and memorize several pass-icons as his password. To login the system, the user have to correctly pass the predetermined number of challenges. In each challenge, the user have to find three pass-icons among a set of randomly icons displayed on the login screen and then click inside the invisible triangle created by those three pass-icons. This scheme also failure. In an another existing technique they provide only circle having eight sector but only having numeric and alphanumeric not a single color in sector and there is no possibility of rotate the sector either clockwise or anticlockwise. This scheme is also not so much secure. After that the new technique is provide and that is nothing but our reference paper technique.

In another existing technique they proposed a scheme as challenge response identification. Means a password in our scheme is time-variant. User who knows the password is able to get the challenge and to respond correctly to the attacker. An attacker still cannot able to tell what the password is, even if he/she has guessed a user's login process. Unfortunately this scheme also occur failure and the password guess by attacker

2. Literature Review

In2002, Sobrado and Birget et al.proposed three shoulder surfing resistant graphical password schemes, first the Movable Frame scheme, second the Intersection scheme and the last one Triangle scheme. However, the Movable Frame scheme and the Intersection scheme have been failure rate. In the Triangle scheme, the user has to choose and memorize several pass-icons as his password. To login the system, the user have to correctly pass the predetermined number of challenges. In each challenge, the user have to find three pass-icons among a set of randomly icons displayed on the login screen and then click inside the invisible triangle created by those three pass-icons. This scheme also failure.

In 2005,L. Sobrado and J.C. Birgetetal. They proposed a scheme as a challenge response identification. Means a password in our scheme is time-variant. User who knows the password is able to get the challenge and to respond correctly to the attacker. An attacker still cannot able to tell what the password is, even if he/she has guess a user's login process. Unfortunately this scheme also occur failure and the password guess by attacker.

In 2006,B. Hartanto, B. Santoso, and S. Welly et al. the movable frame graphical password can only be used for an application that needs better security but does not need a rapid time for the entering password. To overcome this

drawback the replacement of the alphanumerical password with the moveable frame graphical password for the public machine – where most users access it in a very short time – is not recommended yet. Unfortunately this scheme was also fail.

In2009,Gao, X. Liu, S. Wang, H. Liu, and R. Dai et al. proposed a shoulder surfing resistant graphical password scheme, ColorLogin, in which for reducing the login time the background color was usable factor. However, the probability of accidental login of Color Login is too high and the password space is too small. Means hacker can easily guess color of user which he enter as a password and due to that this scheme also high failure.

In 2010,B. R. Cheng, W. C. Ku, and W. P. Chen et al. Asimple text-based shoulder surfing resistant graphical password, in which the user can efficiently and easily complete the login process without worrying about shoulder surfing attacks with the help of sector login.The method of the suggested scheme is simple and easy for users to choose the password first level as a selecting color and second level as a enter text password from the sector which divide into eight sector in circle. But there is also analyses the accidental login.

In 2011, M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar et al. Two authentication techniques based on color and images are proposed for security. Both the techniques use grid for session passwords generation. First level as a color selection and second level as a images selection as a password among multiple images which also occur failure.

In the same year, S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho et al. proposed a text- based shoulder surfing resistant graphical password scheme, and employed an analysis method for accidental login resistance and shoulder surfing resistance to provide the security of their scheme. Unfortunately, the resistance of Kim et al.'s scheme to accidental login is not satisfactory.

In 2013,S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho et al. proposed a authentication level for user to select color and then password among different sector by using key anticlockwise and clockwise for login the system.

3. Proposed Technique

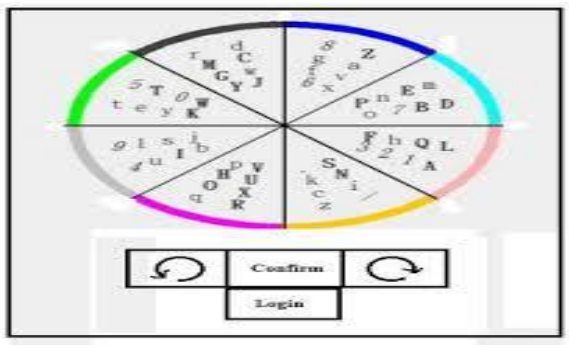

Fig:-1 simple text based shoulder surfing resistant graphical password scheme

In an existing work that is,A simple text based shoulder surfing resistant graphical password scheme, we can see the technique provide for authentication is look like above. One circle provides which divide into eight sector having numeric and alphanumeric into each individual sector. And each individual sector having different color. As seen above there are some key provide for rotate sector to choose color and password either clockwise or anticlockwise and then confirm and login. But anyone can guess this level means someone who is very close to the user then he/she must know the favorites color of user and once the attacker know the entering color of user then he/she is very close to attack the password by guessing attack or dictionary attack. And one drawback is also that this technique only provide for desktop user.

Our proposed technique is that 3D password with session based technique for login security in smart phone. In which we provide two level authentication i,e registration and login.Registration having two stepsfirst whenever mobile user want to use this technique he/she first complete the registration level in which it first enter simple password whatever user want to enter and any one color. And second select 3D password environment and possible object selection on 3D images as a password.

Login level having two steps first login with session scheme in which one circle is occur whenever user going to login and enter his password which select at the time of registration. Here now there is no need to select color. And second step is that login with 3D password scheme. In which user select object on 3D image as a password.

Every time whenever the session is restart the circle which having eight sector with numeric and alphanumeric are shuffle every time likewise the every time whenever new session restart the 3D image is also change. New 3D image will be generated after every session is restart. Because of that the hacker will be confuse. There is no possibility of hacking the 3D image password either if the hacker hack first level password. Because 3D images having more than lack of possibility.

4. Conclusion

Generally we use password either text based or 3D password. If we use only text based password in which the user can easily and efficiently complete the login process but there is some drawback was that guessing attack, dictionary attack and no mobility system. Now our propose technique is that we use two level authentication scheme as a password for mobile user. First level for text based graphical password and next level for 3D image which provide high security to the user. If anyone guess our first level password then there is no possibility to guess our second level password because 3D image will be change whenever the session is restart and hacker will be confused.

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"2013
[2] L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[3] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005.
[4] B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.
[5] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.
[6] B. R. Cheng, W. C. Ku, and W. P. Chen, "An efficient login-recording attack resistant graphical password scheme – SectorLogin," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.
[7] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, May 2011.
[8] S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho. "A new shoulder-surfing resistant password for mobile environments," Proc. of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.