A NOVAL AND EFFICIENT REVOLVING FLYWHEEL PIN ENTRY METHOD RESILIENT TO SHOULDER SURFING ATTACK

Boney Baby[1], Linu Paulose[2]

[1]*M.Tech Student Computer Science and Engineering*
[2]*Asst. Professor, Department of Computer Science and Engineering, Indira Gandhi Institute of Engineering Nellikuzhi, Kerala ,India*

---***---

Abstract -*Authentication based on passwords is used largely for computer application security and privacy. even though, human actions which include c selecting bad passwords and picking passwords in an unstable way are regarded as "the weakest link" in the authentication trail. even if users likely to select passwords either small or understandable for easy remembrance. With internet applications and mobile grows up, people can acquire these web applications anytime and anyplace with different devices. This evolution brings high effect but also increases the reveal passwords to shoulder surfing attacks. Attackers can notice immediately nearby or use external recording devices to collect users' information. To overcome this problem, here proposed a new scheme named revolving flywheel PIN-Entry method to prevent from shoulder-surfing attack. The new scheme holds a revolving flywheel and downward color pad. User will register digits as PIN and for authentication, instead of digits; two color pads will be used to enter digits of PIN. Proposed method is easy to adapt and did not have any cognitive burden. Here implemented this method for mobile terminal and analyzed security, usability and authentication time by experimental survey. This method will be easy to follow by ATM machines or wherever PIN is used for authentication.*

Key Words: **Authentication, Captcha test, Security Questions, QR Code Generation, Fly Wheel PIN Entry**

1. INTRODUCTION

Textual passwords have been used authentication method for years ago. According to the numbers and small and capital letters, textual passwords are used as the powerful enough to prevent against brute force attacks.so, a strong textual password is difficult to remember and recall. According to certain studies shows that humans have a better facility to remember images with long-term memory (LTM). Image-based passwords were tends to be easier to recall in several user studies. According to the result, users can built up a complex authentication password and are capacity to recall it after a long time even if the memory is not initiate periodically.

However, all of these image-based passwords are exposed to shoulder surfing attacks (SSAs). This type of attack may uses direct vision, such as watching someone's shoulder or applies video recording techniques to get passwords, which include PINs, or secure personal information. The human actions include such as selecting bad passwords for new accounts and picking passwords in an unstable way for logins are considered as the weakest link in the authentication trail Says that an authentication scheme should designed to prevent these vulnerabilities.

Nowadays smart phones are restored with computer, laptops and several electronic devices. Smart phones are used for execute transaction, retrieving personal information like emails, contact details, personal data etc. For the security task PIN (Personal identification numbers) are mainly used to lock the smart devices. Large no of graphical and textual authentication methods are organized to resist from shoulder surfing attacks but the challenging problem is that to provide security and usability with less time for authentication task. so that an authentication scheme should always designed to resolve these difficulties.

1.1 Objective

The objective of this thesis is to proposed a new scheme named revolving flywheel PIN-Entry method to prevent from shoulder-surfing attack. The new scheme holds a revolving flywheel and downward colour pad. User will register digits as PIN and for authentication, instead of digits; two colour pad will be used to enter digits of PIN. Proposed method is easy to adapt and did not have any cognitive burden. Here implemented this method for mobile terminal an analysed security, usability and authentication time by experimental survey. This method will be easy to follow by ATM machines or wherever PIN is used for authentication.

2. BACKGROUND AND RELATED WORK

In the past decades, a large no of research on password authentication has been already done in the literature. Out of these proposed system, this paper focuses mostly on the graphical-based authentication systems. To keep this paper short, it will give a compressed analysis of the most related schemes that were declared in the earlier section. so many other schemes may have good usability but they are not always graphical-based and always need extra support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc. In the past days, the graphical capacity of handheld devices was weak that meanie the color and pixel it could show was narrow.

Under this limitation, the Draw-a-Secret (DAS) techniques were introduced by Jermyn et al. in 1999, where the user is tends to re-draw a pre-defined picture on a 2D grid. It directly draws out the figure. If the drawing touches the same grids in the same sequence, so that then the user will be authenticated. Since then, the graphical capacity of handheld devices has steadily and ceaselessly become better with the advances in science and technology. In 2005, Wiedenbeck et al. propose a graphical authentication scheme PassPoints, and on at that time, handheld devices can a shown high resolution color pictures.

Using the PassPoint scheme, the user want to click on a set of predefined selected pixels on the predestined photo with a correct sequence and within their squares during the login stage. After that Martinez-Diaz et al. also expand the DAS based on finger-drawn doodles and pseudo signatures in most mobile device. This authentication system is form on features which are extracted from drawing process (e.g., speed or acceleration). These features contain behavioral biometric characteristic. So here says that the attacker would have to follow not only the user draws, but also how the user want draws it. So, these three authentication schemes are still all exposed to shoulder surfing attacks as they may tell the graphical passwords directly to some stranger observers in public place.

According to the graphical authentication schemes, there was seen some research on the extension of personal identification number (PIN) entry authentication systems. In 2004, Roth et al organize an approach for PIN entry resilient toward shoulder surfing attacks by increasing huge noise to observers. In their schema, the PIN digits are shown in black or white randomly in all round. The user must reply to the system by getting identified the color for each password digit. After that the user has made a series of binary choices (black or white), the system can show out the PIN number the user tends to enter by looking the user's choices.

This method can confuse the observers if they watch the screen without any help of video recording devices. Even if observers are able to take the whole authentic In order to prevent the shoulder surfing attacks with video capturing, FakePointer was proposed in 2008 by Takada. In the usage of FakePointer,it contain PIN number, where the user would get a new "answer indicator" each time for the authentication process at a bank ATM. In other way, the user must need two secrets for authentication: a PIN as kept as fixed secret and an answer indicator is also as a disposable secret.in the process, the passwords could be cracked easily so that the answer indicator is a form of arranged in n shapes if the PIN had n digits

3. SYSTEM OVERVIEW

The purpose of Revolving Flywheel authentication method is satisfied by considering on parameters such as security, usability and time.

- Security: System must be quite dependable for any shoulder surfing attack, there will be no matter whatever it is password theft or camera based recording.
- Usability: System must be user companion so that any person can use with fun and easy mood.
- Time: It must take minimum time for authentication process.

Proposed method is consist of the following components such as

- QR Code Generation
- Captcha Test
- Revolving Flywheel PIN Entry Method
- Communication Module
- Password Verification Module
- Database

QR Code Generation-QR codes are in the form of 2 dimensional matrixes. It will store a large volume of unique data. Steganography technique can be used to hide the data in the form of an image or text. in the modern word data can be digital image, Video or Audio file. This module encrypt PIN no and EPIN no will be hide in the form QR code, it will be sent to users mail id using QR scanner PIN no will be decrypted.

Captcha Test- there will visual authentication scheme with secure layers for desktops or laptops are used. The main layer will be recognition-based scheme that addresses always the human factors for recognizing a Captcha and images with specific patterns. The proposed authentication system is powerful against brute-force, The proposed scheme usability was tested by using the Computer System Usability Questionnaires, so that the result will be highly usable and could improve the security level on ATM machines. This module is used in order to recognize user or Robot.

Revolving Flywheel PIN Entry Method- In this module a revolving fly wheel lock screen will be shown. Revolving wheel composed of three layers and ten sectors and thirty sections. Set the number in the middle layer of each section randomly and also Fill the colours in each of the layers. When user will enter input for first time then the revolving wheel will revolve in clockwise direction. User will see the colours associated with the inside and outside layers of the number of his PIN and will click the button accordingly. Continue the step for every number of the user PIN. There will be session time is also allocated , if user failed to login then warning message will be sent to user mail id Security Question will be provided to continue the login section If failed to answer then login section will be closed. Users can also get device login detail by sending SIM and IMEI no to the server using hashing function. After completing successfully login process, enter into Online banking and certain transaction process can be done.

Communication Module- In this module it can transmit information between the client devices and the authentication server. Any communication can be protected by SSL (Secure Socket Layer) protocol and thus, it will be safe from being eavesdropped and intercepted.

Password Verification Module- This module check the user password during the authentication phase. The user is authenticated only if PIN no is correctly got in.

Database- The database server contains numerous tables that store user accounts, passwords and the time duration on each user spent on both registration phase and login phase. Information about PIN no in the database will be encrypted form. Users can also get device login detail by sending SIM and IMEI no to the server using hashing function.

3.1 Revolving Flywheel PIN Entry Method

Revolving Flywheel PIN entry Method consists of a registration phase and an authentication phase as described below

Registration Phase

- At this stage, personal details will be entered and choose two colours for pin no after that it will be sent to the server.
  - ➢ At the server ,after getting all the details ,it will generate a PIN no and this PIN no will be encrypted
  - ➢ Then convert encrypted PIN into QR code and mail QR code to user.
  - ➢ After that scan QR code, if it is valid then enter into login page. If it fail then it failed to register.

Authentication Phase

- At this stage User uses username, password after that there will be captche test, to recognize whether it is user or robot.
- After that a revolving fly wheel lock screen will be displayed.
- Revolving wheel consist of three layers and ten sectors and thirty section
- Put the number in the middle layer of each section randomly.
- Fill the colors in each of the layers.
- When user will enter input for first time then the revolving wheel will revolve in clockwise direction.
- User will see the colors associated with the inside and outside layers of the number of his PIN and will click the button accordingly.
- Continue the step for every number of the user PIN.
- There will be session time is also allocated, if user failed to login then warning message will be sent to user mail id.
- Security Question will be provided to continue the login section
- If failed to answer then login section will be closed
- Users can also get device login detail by sending SIM and IMEI no to the server using hashing function.
- After completing successfully login process, enter into Online banking and certain transaction process can be done.

4. CONCLUSION

With tending use of web services and apps, users can able to access these applications anytime and anyplace with different devices. In order to hide users‟ personal property , authentication must be required every step for every time when they try to access their personal account and data.so that organizing the authentication process may result the shoulder surfing attacks. Even a complicated password can be easily followed through shoulder surfing.To overcome this problem, here proposed a new scheme named revolving flywheel PIN-Entry method to prevent from shoulder-surfing attack.

The new scheme holds a revolving flywheel and downward color pad. User will register digits as PIN and for authentication, instead of digits, two color pad will be used to enter digits of PIN. Proposed method is easy to adapt and did not have any cognitive burden. Here implemented this method for mobile application and access security, usability and authentication time can be evaluated by experimental survey. This method will be easy to follow by ATM machines

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authenticationschemes: Current status and key issues," in Proc. Int. Conf. Methods Models

Comput. Sci., Dec. 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphicalpasswordauthentication: Cloud securing scheme," in Proc. Int. Conf.Electron.Syst., Signal Process. Comput. Technol., Jan. 2014, pp. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld,May,vol.9,20052556096/security0/biometrics–getting-back-to-business.html

[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proc. 9th Conf. USENIX Security Symp.-Vol. 9, 2000, pp. 4–4

[5] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints:Design and longitudinal evaluation of a graphical password system," Int. J. Human-Comput. Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[6] Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Sci., vol. PS-11, pp. 137–138, 1968.

[7] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," J. Exp.Psychol.: Human Learn. Memory, vol. 3, pp. 485–497, 1977.