MOBILE APP AUTHENTICATION TO IMPROVE SECURITY IN ANDROID DEVICES

A.Pradeep[1], A.Sandeep[2], D.Vanitha[3], R.K. Kapilavani[4],

[1, 2] *Student,* [3, 4] *Assistant Professor,*

[1, 2, 4,] *Department of Computer Science and Engineering,* [3] *Department of Information Technology,*

[1, 2, 3,] *Prince Shri Venkateshwara Padmavathy Engineering College,*

[4]*, Prince Dr.K. Vasudevan College of Engineering and Technology,*

[1,2,3,4,] *Tamil Nadu, India.*

Abstract

Secure Authentication is very important in today's digital world, Mobile devices use sophisticated applications that makes life easier and more relax and convenient for users. Mobiles are the database for any person's personal information. Therefore it turns as an attractive target for the spyware injections. Such malware software's can steal the user's credentials and valuable information's from their accounts. The main aim of this project is to propose the smart way authentication by using a unique logic on authentication and by using screen brightness of android mobiles in order to avoid spyware attack, shoulder surfing attack, and man-in-the-middle attack.

Keywords – *Authentication, screen brightness, android, spyware, shoulder surfing, man-in-the-middle, interfacing layer.*

1. INTRODUCTION

The Smartest way to authenticate in today's digital world is very important as the mobile devices stands as a database for the user's personal information's in many social media networking. Smartphone's provide space to sophisticated applications development that makes user's more relax and convenient. There are many authentication schemes proposed to overcome the attacks done but each of it provides its own drawbacks, some of the attacks that are at most undetected are shoulder surfing attack, spyware attacks, and man-in-the-middle attack.

The Existing system uses One-factor Authentication and Two-factor Authentication mechanisms, where the one-factor authentication is the traditional user authentication providing User Id and a password, the two-factor authentication included an additional physical token along with the one-factor authentication (i.e.) the user Id and password. Many online social websites today use one-factor authentication as their authentication procedure to secure the individual users profile because of managing the physical tokens or biometric information cannot be easily and practically implemented as of today available devices commonly available in the market. Generally bank authentication following two-factor authentication includes a card as physical token and biometric information's but these social Medias uses OTP generation, user browser details and additional security questions etc. There are lots of huge databases carrying redundant information's about user's personal information such as security questions.

The scale for security has increased rapidly due to the machine learning and automated bots that are used to crack the authentication process, to distinguish between a computer bot and a human, some complex cognitive intelligence test, for example CAPTCHA can be implemented. But the drawback of these CAPTCHA is it slowdowns the authentication process and user hates these mechanisms, hence low level of acceptance among users.

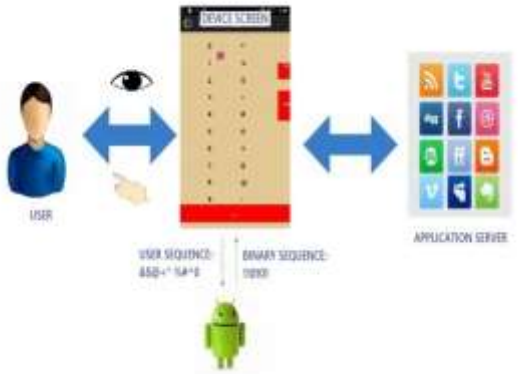


Figure 1 Proposed Authentication concept

In this paper the proposed system is about providing a safer authentication method that using a unique interface representation for entering PIN and using screen brightness of the mobile devices as shown in figure 1. This proposed system prevents user credential details identified by the spyware injection, also avoids shoulder surfing and man-in-the-middle attack. The interface element consist of a vertical column where digits from 0 to 9 are displayed and another column consisting of random symbols such as +, /, etc. And the brightness factor is implemented as it is stated in M.Guerar et al [1], the brightness factor is to add complex data for the spyware intruders. The Base64 algorithm and Hmac algorithms are used to provide encryption and signature values to prevent information's from man-in-the-middle attack. Hence this paper provides a highly secured user authentication scheme that is ease of use to the users.

2. RELATED WORK

Trending world having a varieties of mobile operating systems, that are capable of running various applications both at the front end and the background. Apart from the ordinary phone functionalities additional sensors are embedded in Smartphone's, which provides high interface experience for the user. There are many papers proposed to safeguard the credentials of the user during authentication such as PassWindow by Yi[2], FakePIN [3] and spyware resistant user authentication scheme proposed by kim[4].

In order to provide a safer authentication scheme, Let us refer how the passwords can be inferred during authentication process.

Simon. L, et al. [5] proposed PIN Skimmer, which inferences the password during authentication with the help of camera and the microphone in the user device. Android OS has the shared resources permissions capable of sharing information's by the app running in the background. It collects the photos of the user during authentication and sends those images to the server, there image processing is done, identifying the angle and position differences of the image whenever a button pressed. With the results of these processes the users PIN is identified.

Owusu. Z, et al.[6] proposed ACCessory, where the password is inferred with the help of accelerometers in the mobile devices. Whenever the authentication process takes place the readings of the accelerometers are processed to identify which parts of the screen are pressed. TouchLogger is an app that is similar to this system that is available in the market stores.

Figure 2 Screen captured when brightness is low and when brightness is high

Xu. Z, et al.[7] proposed TapLogger, here the on-board motion sensors are used to infer the input data's that are given to the phone. The touch screen of Smartphone's work on the flow of electron volts over the screen and whenever user touch at that particular region there is a voltage drop recognizing the x, y coordinates of the screen, from this way these data's are sent to the server by the background running app. Hence the inputs of the user during authentication can be inferred.

Shoulder-surfing attack is one of the common attacks that are undetectable by the device. To prevent this attack some interfacing layers can be used as suggested by kim in his user authentication scheme.

These are some of the ways how password is being inferred from the devices and the other part is generating computer bots to break this password using machine learning and specific algorithms. To identify human and computer bots, CAPTCHAs have been introduced and most users hate CAPTCHA for it takes long time during authentication, hence it is omitted and the restriction of entering wrong passwords is limited and the account is locked when maximum limit count is reached[8].

Another scenario of password theft is occurred by man-in-the-middle attack again it is undetectable by the device, while spoofing over the message is done. Even though the probability of crypt analyzing is low, chances of identifying the characters are there, so it cannot be restricted but can be made more complex with the logical thinking by sending a set of characters that together resembles the password.

From this kind of malware application to prevent ourselves by preventing password thefts we introduce a new authentication mechanism based on unique logical representation and brightness factor of the mobile device, overcoming the limitations of all the spyware injections and ease of use for the users.

3. AUTHENTICATION METHODOLOGY

This logic based authentication is through visual mapping of symbols along with the digits preventing the undetectable attacks by the devices. Furthermore the implementation of this authentication is going to be in android devices.

3.1 **Account creation and password registration**

Figure 3 Screen captured for all 6 rounds during Authentication

The account creation for social media networking is generally of username, email-ID, date of birth, etc. In the proposed system it is similar to the account created in social media but the PIN (personal identification number) is generated by the server and mailed to the registered email-ID. In this way the PIN generated by the server is no way related to the user's personal information providing further safety for the account owner from unauthorized entries. The account creation phase is normal and here too the user dint enter the password directly as it is generated by the server preventing the data's from the malware software.

3.2 User Validation

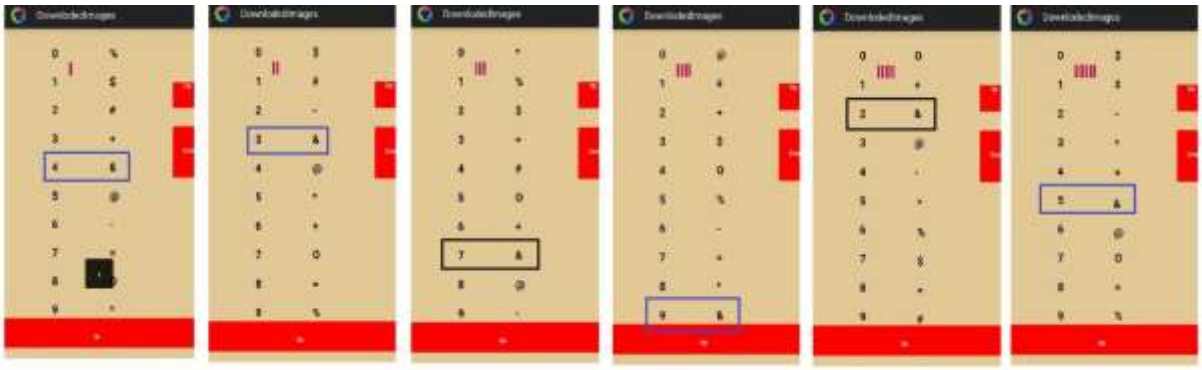
User Validation is an important part in preventing shoulder surfing attack and spyware injections. As Validation is a process of providing the user known value to prove his identity this step is to be designed carefully. The proposed system uses an interactive user interface for entering the PIN using symbol representations to enter the PIN. The validation phase is going to be of N rounds where N>2, this validation phase uses the brightness factor [1] to avoid spyware attack and the symbol interface is used to avoid the shoulder surfing attacks. It is a PIN-entry method. The Interacting interface design along with the brightness factor has the layout design that consist of ten objects arranged randomly in a vertical order placed accordingly to the digits that are permanent on the left side of the screen and the objects are moveable in the vertical order using the up and down buttons as shown in the figure3. The figure3 shows six continuous next to next screen during the authentication process. The first interface layout with the symbols displayed during the brightness level high is the key discussion round for that particular session as the keys are decided at the instance of authentication. After the first round when the key is decided then in the consecutive rounds of screen brightness high enter the second digit, third digit of the PIN and so on. At the end of the each round assign the inputs through the up and down keys and press "OK".

Spyware attack will be avoided by proposing the idea that uses the screen brightness as an authentication tool. The android secure element generates the 6 digit binary value. Based on the binary digit the brightness of the screen gets changed to high or low. If the screen brightness is high the user should input the correct PIN digit. Else the user can skip the screen or assign a random input. From example shown in the figure 4, considering the brightness factor as the difference of the images the screen shots of images cannot be identified when brightness level low and high is shown here, where the PIN is 4395, the user recognizes symbol as the session key because it is collocated with the first digit of the PIN, 4. In the next rounds it is a normal PIN-entry round, in which the each consecutive rounds when brightness is high the session key should be assigned for 3, 9 and 5. In each of these rounds, the user enters a PIN digit in its sequence by aligning the session key aside the array of ten digits arranged randomly in a vertical manner.

3.3 Authentication

After the user validation process the proposed system will remove the digits which inserted while the screen brightness is low and apply the Hmac algorithm for the PIN given by the user and generate the Signature for the user PIN which is digestible value in order to avoid Man-in-the-middle attack. The server get the signature of user generated PIN and generate the signature value for the Original PIN and compare two signatures. If the signatures are equal the user can access the profile of the user. If not user can't access the profile. Here instead of passing the password digits directly the array of symbols during brightness level high is passed along with

Figure 4 Highlighted for "&" as key for PIN 4395 with Brightness value 110101



encryption and signature values. On receiving these symbols the server identifies the exact positions of the PIN fields and if all the particular fields hold the same symbol or object, then the user is authenticated.

3.4 Overall Concept

Mobile social network requires a higher level of security provides to enhance and secure classic widespread PIN authentication method. So the proposed system uses a *logical interface screen and lie overhead* concepts.

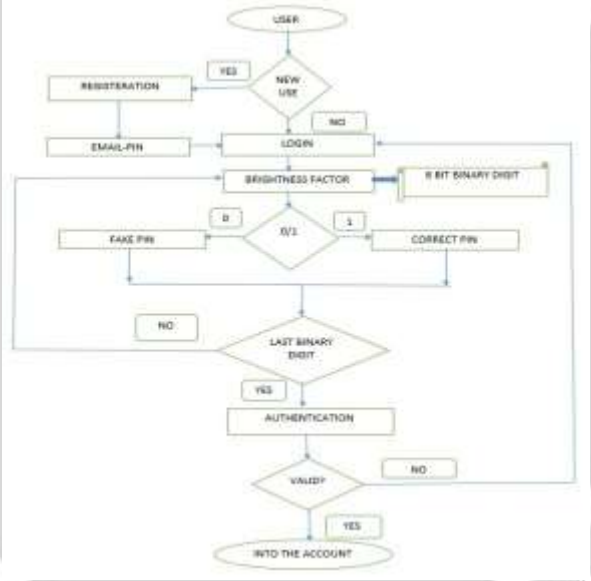


Figure 5 System Flow

This idea is about mapping symbol along with digits along with some fake input values. The authentication process involves entering the PIN with different interface without directly entering the digit in the screen instead only scroll buttons are pressed to align the symbols according to the password. The session key is going to be decided only at the time of authentication for that particular instance hence this prevents shoulder surfing attack and the use of lie overhead concept by adding some fake values that is distinguishable by the user during logging in.

Because of this overall complexity of logical and lie overhead concept the strength of the authentication is improved. Considering the example in the figure 4, the PIN 4395 is entered with the brightness factor of six digit binary value that consists of four 1's and to 0's generated randomly, in this instance it is 110101. So the key used in this session is "&" and it is hard to identify the key or password even though spyware injections takes place.

The Activity flow of the proposed system can be stated as follows according to the figure 5.

- New user needs to create account and register password.
- If not new user it lets into the authentication process.
- If brightness is low enter a fake pin or skip the tab by pressing ok.
- Else if brightness is high enter the correct pin mapped with the session key.
- Repeat the previous process until last binary value is reached.
- Removes the fake pin and sends the symbols with signature values to authenticate the user.
- The server confirms the validity of the user and lets into the account.

This provides an improved security the use case of this process is explained with the example that is shown in the figure 4. Without the box that is highlighted it is not possible to identify the PIN of the user. And the lie overhead further increases the complexity of during the password inference by spyware injections, the lie overhead values are represented by black box in the figure 4.

4 SECURITY ANALYSIS

The security analysis is about how the proposed system overcomes the spyware recording attacks, brute force attacks, side channel attacks and theft of Smartphone.

4.1 Spyware recording attacks

As this proposed system avoids the shoulder surfing attack it also prevents the spyware but on repeated viewing of the authentication it is possible to predict the closer pattern hence the idea that uses the screen brightness as an authentication tool is used to avoid this issue. Since the user is not directly letting the inputs this proposed system over comes the spyware recording attacks.

Again let us look into the example as shown in the figure 3. To prove that the proposed system overcome the spyware recording attack, looking into the recorded screen every digit is assigned with an symbol along with the lie overhead hence it is impossible to infer the PIN during authentication in this system.

4.2 Brute Force attack

Brute Force attack is by entering all the possible entries into the PIN and identifying the PIN. The brute force and dictionary attacks can also be tried together, dictionary attack is the attack that uses the frequently entered input as the passwords in the device but as the session key is decided during at the particular instance and along with the brightness factor it is not possible to infer the passwords using the brute force and dictionary attacks.

4.3 Side channel attack

The side channel attack uses the shared resources that are available to the background running app such as the accelerometer, on-board motion sensors, camera, gyroscope, and microphones.

These attacks are done by getting access for the shared resources. During the authentication process the background running app records and collects its appropriate values. There are various modes in side channel attacks, such as monitoring mode, collecting mode, learning mode and logging mode. The monitoring mode monitors the device process and collects the data during authentication takes place, this later part is done in the collection mode and sent to the dedicated server for the pin inferring systems, with the collected data's the server process the data and gets information about the password details, this mode is called learning mode and logging mode is the intruding into the unauthorized account by the password theft.

But these side channel attacks are restricted in our proposed system by the use of restricted dedicated buttons to enter the pin and since there is limited space allocated for the user to input the PIN, the complexity task for the side channel attacks to infer the passwords has the probability value highly close to zero.

Hence the proposed system has improved security and ease of access for user authentication that the existing authentication systems proposed.

4.4 Smartphone theft

Even though if the theft of smart phone occurs, it is impossible to access into the user account until unless the PIN is known by the unauthorized person. Because the authentication should be done for every successful login without which, no one can gain access into the users account. Hence the account is preserved and authentication improved security prevents the user data every time in the worst case of theft of Smartphone's.

From these overall scenarios of security analysis made, the proposed system has high resistant strength against all the malware injections and attacks made to infer the user's credentials. And also it is conveniently ease for people to login easily without fear of password leakage.

5 CONCLUSION

The main problem identified and proposed a system to overcome the problem is, in day-to-day digital life every person mobile are serving as the database of their personal information's. So the spyware injectors are targeting the mobile devices, these Smart phones are used for gaining access often vulnerable to many kind of malware attacks that can be able to retrieve data such as PIN codes and passwords as they are inserted to perform authentication to the target social networking applications.

Therefore the proposed system uses a unique logic based and brightness based authentication mechanism capable of enhancing the security of identity confirmation PIN codes without the need for the user to remember an additional confidential value or to solve an arithmetic or visual cognitive task. This method introduces a new input value that is dynamic at every usage assigning a PIN with an interface element that cannot be captured by spyware.

Thus the proposed system has the characteristics of user friendly and the interactive environment for the user, eliminating the shoulder surfing attack and Man-in-the-middle attack has been neglected by using hmac algorithm by generating digested hash value for the user PIN.

We implemented a smart way to authenticate the social networking accounts belonging to them by using a logical based interface and screen brightness of mobile device in order to avoid the spyware attack, shoulder surfing attack, and man-in-the-middle attack.

REFERENCES

[1] Guerar M, Migliard M, Merlo A, Benmohammed M, Palmieri F, Castiglion A, "Using screen brightness to improve security in mobile social network access" IEEE DOI:10.1109/TDSC.2016.2601603

[2] Yi H, Piao Y, Yi J.H: Touch logger resistant mobile authentication scheme using multimodal sensors. In: Advances in computer science and its applications, Volume 279 of lecture notes in Electrical Engineering, pp.19-26, Springer, Berlin (2014).

[3] Kim S, Yi H,Yi J.H: FakePIN: Dummy key based mobile user authentication scheme. In Ubiquitous Information Technologies and applications, volume 280 of lecture notes in Electrical Engineering pp. 157-164, Springer, Berlin (2014).

[4] Kim T, Yi, J.H, Seo C: Spyware resistant smartphone user authentication scheme. DOI:10.1155/2014/237125

[5] Simon L, Anderson R: PIN Skimmer: Inferring PINs through the camera and microphone.DOI:10.1145/2516760.2516770

[6] Owusu E, Han J, Das S, Perring A, Zhang J: ACCessory: password inference using accelerometers on Smartphone. DOI:10.1145/2162081.2162095

[7] Xu Z, Bai K, Zhu S: Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors.DOI:10.1145/2185448.2185465

[8] Reynaga G, Chiasson S: The usability of Capthchas on Smartphone's. In: Proceedings of SECRYPT pp.427-434, SciTePress (2013).