IMPROVING SECURITY IN MOBILE NETWORK ACCESS USING SCREEN BRIGHTNESS AND SYMBOLS

Mrs.S.Irin Sherly, K.Abirami, M.Amoka and T.E.Kalaivani

irinkutty@gmail.com, abi15051996@gmail.com , amoka.karthika.81195@gmail.com , tekalaivani@gmail.com

***Abstract*—In today's mobile communications scenario, smartphones offer new capabilities to develop sophisticated applications that make daily life easier and more convenient for users. Such applications may involve mobile ticketing, identification, access control operations, online transactions etc., are often accessible through social network aggregators. The modern smartphones are very powerful devices but it also makes them very attractive targets for spyware injection. This kind of malware is able to bypass classic authentication measures and steal user credentials even when a secure element is used, and perform unauthorized mobile access to social network services without the user's consent. Such an event allows stealing the sensitive information or a full identity theft. In this work, we address this issue by introducing Bright Pass which is a novel authentication mechanism based on screen brightness. Bright Pass allows users to authenticate with a PIN based confirmation in the presence of specific operations on randomly arranged objects (i.e. ., symbols). Furthermore, we empirically assess the security of Bright Pass through experimentation. Our tests indicate that Bright Pass and symbols protects the PIN code against automatic submissions carried out by malware while granting fast authentication phases and reduced error rates.**

Index Terms— Authentication, Brightness, Malware, Mobile-Access, Smartphone, Social Networks, Usable security.

I .INTRODUCTION

In the last years, social network providers are more focused on attracting users and building large warehouses of personal information than on securing the access to the infrastructures. The active users of social networks available on the Internet now aggregate to several billion people and mostly use the mobile devices, such as smartphones or tablets, to access the provided services. Many of these users now consider social networks as the preferred way to manage their personal data, and use their social network access credentials to simplify and manage their various profiles and accounts on many service portals. Unfortunately, as the strategic importance of these platform raises, the interest of the hackers increases , that leads to identity theft , authentication breaches and aiming at several hostile activities , become fundamental problems in the social networking arena, lying at the basis of most critical security challenges.

Many attacks are successful in accessing to social network accounts since the password-based authentication paradigms are not efficient and robust enough, hence they are vulnerable to automated attacks.

A recent study from LinkedIn and Twitter hacks confirms that weak passwords and single factor authentication are still the main security weaknesses in most social networking sites. Accordingly, two-factor authentication seems to be the simple and most effective protection strategies of currently available. Many of the topmost social networking services providers such as Google, Yahoo, Facebook , Twitter, Drop box and Snap chat already allow you to optionally require second authentication.

However, the traditional two-factor authentication mechanisms are not applicable to social networks because physical token or biometric data cannot be easily log into users' profiles. The alternative is complementing the single factor (password-based) authentication process with additional identification elements, such as one-time PIN codes, generated by the user's own device (e.g. the smartphone) or received via SMS. Unfortunately, the mobile devices used for gaining access are vulnerable to several kinds of malware which retrieves data such as passwords and PIN codes when they are inserted to perform authentication on the target social network applications. Hence, the presence of such malware in the mobile platforms can seriously impact the user's privacy and security, reducing the user's trust on social network services.

In this paper, the brightness based authentication mechanism (i.e., Bright Pass) capable of enhancing the security of identity confirmation PIN codes without asking the user to memorize any additional secret value or to solve a complex cognitive task. This method introduces a new input value that is changed at every usage combining a PIN number which is known with an interface element that cannot be captured by spyware, i.e., a phone screen will increase the brightness to tell the user when to enter the correct PIN digit and when to enter a fake one.

Unlike the existing authentication schemes, the Bright Pass does not prevent the spyware from stealing the user's PIN code. On the contrary, it prevents the malware from correctly inserting PIN code, thereby disallowing the possibility in performing critical operations without the user's agreement. Our work, show that Bright Pass provides adequate security for mobile devices and sensitive applications against different types of spyware that deals

with user authentication. Thereby, the Bright Pass can increase user confidence to access social networks.

II.RELATED WORK

Today's smartphones are built on advanced mobile operating systems that allow them to run applications with the rich functionalities. Most of them are equipped with new communication interfaces that allow smartphones to carry out security-critical operations which can access sensitive personal data in social network applications. Most of the applications running on these devices still using static alphanumeric passwords or PIN codes as a mean of authentication in accessing sensitive data or performing critical transactions, even though these methods are exposed to spyware attacks. Users easily access marketplaces and choose the applications to install on their smartphones.

Unluckily, this system also leads to the possibility for mobile malware to spread across online marketplaces and fool the user. For these reasons, users may end up installing such applications without realizing that they may include spyware able to track all activities and authentication transactions carried out in their devices. This can be done by using side-channel attacks [1], or by more advanced forms of spyware that are able to record the entire authentication screen along with the user's touch coordinates, and then password is stolen by processing the recorded data and perform unwanted operations on the social platform without the user's awareness. This approach relies on preventing the spyware from stealing the user's credential.

Yi et al. [2] proposed PassWindow, an authentication method which use PIN digits and a pre-selected image calledPass-icon as the password. The basic idea behind this system is to display the Pass-icon to the user with other randomly selected decoy icons on a graphical grid called Pass-Window. The user has to memorize the pass-location that is the pass-icon location within the pass-window.

Afterward, the virtual keypad in addition to the pass-window appears in the center of the screen without its images. To authenticate, the user has to move the pass-window on the virtual keypad by angling it in such a way that the pass-location moves over the PIN.

The user has to cover the rear camera lens with a finger while entering each digit to hide the input. Thus, it prevents shoulder surfing attacks and the security against side channel attacks is increased and its user study shows that the authentication speed is very low.

Kim et al. [3] proposed a password authentication scheme based on dummy-key, called Fake PIN. In this scheme, the password consists of an alphanumeric text and a password direction as an additional secret value. During login, instead of directly inserting the original password, the user has to combine password and password direction in order to fool the observer by pressing a fake dummy key value. Since the location of the keypad letters is changed randomly for each authentication, an attacker fails to authenticate with the password acquired by shoulder-surfing or side channel attacks.

Recently, Kim et al. designed a recall-based graphical password for mobile devices, which is resistant to spyware attacks. Their approach is based on three elements: arrows in the same direction, the omission of authentication values and the random errors inclusion. The user has to memorize the password's location in a 5 * 7 grid. While logging in, the user selects cells according to the arrows displayed in each password's cell whereas the starting cell position changes randomly each time. This method ensures security against side-channel attacks and spyware attacks. However, while including errors the security of this scheme is increased, this study shows that it decreases its usability.

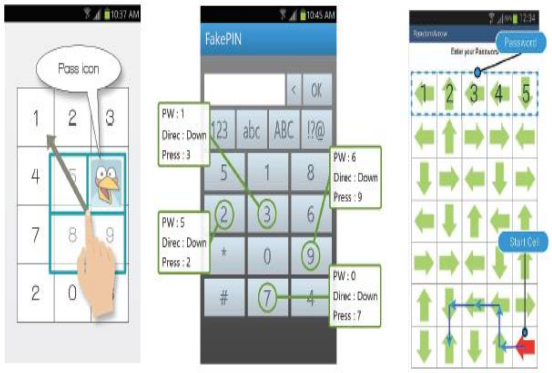


Figure 1: PassWindow, FakePIN and Kim et al.'s scheme.

The security against automated attacks is increased by asking users to solve challenge-response tests such as CAPTCHA before allowing them to enter their PIN/password. The most widely-used form of CAPTCHA is text based where distorted texts are shown as CAPTCHA images. ReCAPTCHA is designed by Ahn et al [4]. Their approach consists of using scanned words from old books that are not recognized by Optical Character Recognition (OCR) program.

However, the hardest type of this scheme has been recently broken by Goodfellow et al. [5] using neural networks. In addition to security issue, a recent research pointed out that existing schemes of CAPTCHA, including reCAPTCHA, are not appropriate for mobile devices. This is due to important usability problems that frustrate users and lead to errors. In[6], authors suggested another input mechanisms aimed at improving the usability of ReCaptcha on smartphones. However, the results of their user study shows that the participants prefer the existing ReCaptcha scheme, that uses the virtual keyboard as primary input.

Chow et al. [7] introduced the idea of showing several textual CAPTCHAs into a grid of clickable CAPTCHAs. Their system does not rely on keyboard input, which can be particularly irritating on mobile devices.

Instead, the user is asked to select some elements in the grid that match the challenge requirement. Inspite of showing some advantages, this scheme has not been widely deployed.An another type of text-based CAPTCHA forms are image based CAPTCHAs. A typical CAPTCHA of this kind is Asirra [8] that displays 12 images of cats and dogs and asks users to select all cat images among them. Their user study shows that time taken for solving the Asirra challenge is 30 seconds for 96.6% of humans which is advantageous compared to text-based CAPTCHAs.

Shirali-Shahreza et al. [9] proposed CAPTCHA mechanism for smart Mobile devices, called Drawing CAPTCHA. In this method, several dots are displayed on a screen with a noisy background. The user has to connect specific dots to each other to pass the CAPTCHA challenge. It is not secured.

Another form of CAPTCHA that has been introduced in recent years is game-based CAPTCHA. Liao et al. [10] proposedaccCAPTCHA, a new CAPTCHA scheme for mobile device based on game logic and human recognition. In this scheme, the user has to play a simple rolling ball game.However; the user study shows that most of the games take a more time to pass the challenge (e.g. stack game 47.3 sec, rolling ball game 25.2 sec and Racing game 55 sec).

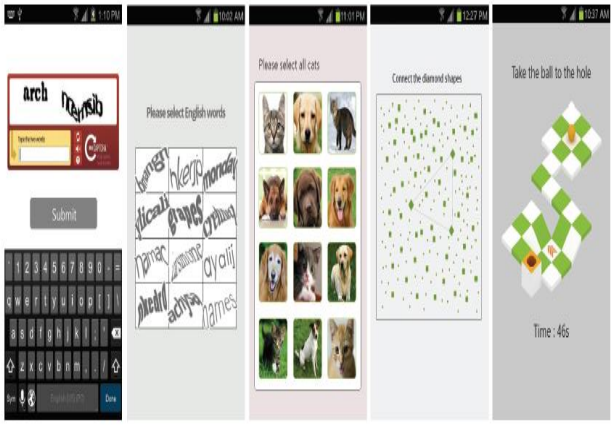


Figure 2: ReCAPTCHA, Clikable CAPTCHA, Asirra, Drawing CAPTCHA and accCAPTCHA.

III. PROPOSED WORK

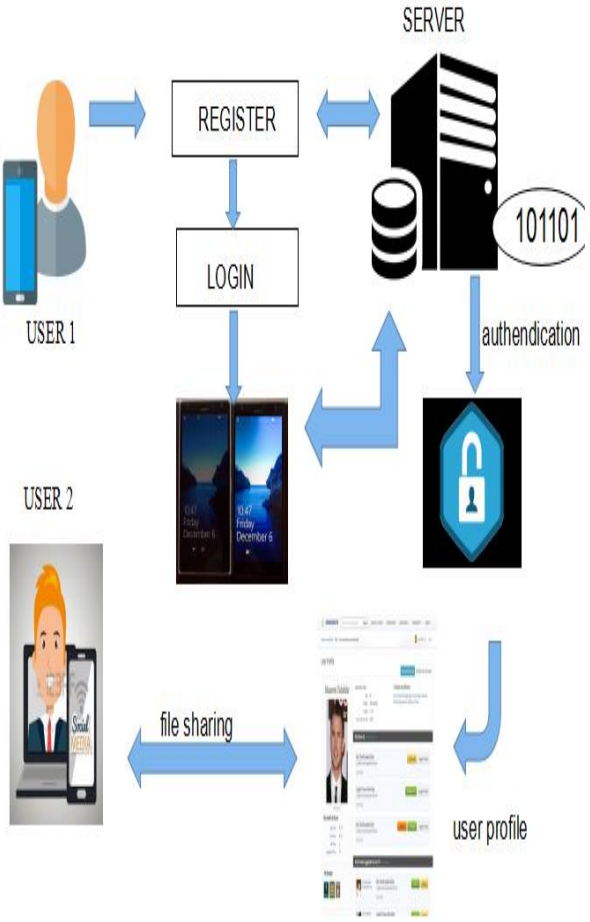
We propose a brightness based authentication mechanism (i.e., Bright Pass) capable of enhancing the security of identity confirmation PIN codes. The android secure environment generates the 6 digit binary value. Based on the binary digit the brightness of the screen gets changed to high or low. If the screen brightness is high the user should input the correct PIN digit. Else the user should give the wrong and random PIN number. Unlike the existing authentication schemes, Bright Pass does not prevent the spyware from stealing the user's PIN code. On the c1ontrary, it prevents the malware from correctly inserting the PIN code, thereby disallowing the possibility to perform critical operations. Thereby, Bright Pass can increase user confidence in accessing social networks. Our project shows that Bright Pass does not hamper usability and provides adequate security for mobile and sensitive applications against different types of spyware that deal with user authentication. Our scheme has a level of flexibility to attacks that makes it usable as a second level of authentication to guard especially sensitive data and operation.

IV.ARCHITECTURE DIAGRAM

V. SECURITY ANALYSIS

In this section, the security of the Bright Pass against shoulder surfing attack, spyware attack and man in middle attack.

A. Shoulder surfing attack



In computer security, shoulder surfing attack refers to in using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data (e.g. Entering PIN in ATM machine).In the proposed system, a new PIN-entry method is used. The basic layout of our method comprises a vertical array of digits from 0 to 9, with another array at adjacent of ten familiar objects such as + and / etc. For simplicity, we assume the number of digits in a PIN is four, and the proposed method may be applied to any case with $N \geq 2$ digits. There are a total of four rounds. The first round is the session key decision round and the remaining three rounds are PIN-entry rounds. In session key decision round, ten randomly arranged symbols are displayed to the user. The user recognizes the symbol immediately below the first digit of his/her PIN as temporary session key and presses "OK." In the example shown where the PIN is 3712, the user recognizes symbol as the session key because it is collocated with the first digit of the PIN, 3. The remaining rounds are PIN-entry rounds, in which the i th digit of the PIN is entered in i th round for i = 2, 3, 4. In each of these rounds, the user is again given a random array of ten symbols, and he/she enters a PIN digit by rotating object array and aligning the session key with the current PIN digit. For this task, the user can use two additional Buttons ("Left" and "Right") to align the symbol with current PIN digit.

B. Spyware attack

Spyware is a type of malware which is installed on a computer without the knowledge of the owner in order to collect the owner's private and sensitive information. Spyware is often hidden from the user to gather information about interactions, keystrokes or keylogging, passwords, banking credentials and credit card details and other valuable data and send them over the internet to hackers. The purpose of spyware is to secretly record what you do on your computer .spyware can also be used some legitimate **purposes** but the majority of **spyware** is malicious.

We have avoided spyware attack by proposing the idea is to use the screen brightness as an authentication tool. The android secure environment 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 should give the wrong and random PIN number.

C. Man in middle attack

A man-in-the-middle attack is a type of cyber-attack where a malicious actor or the intruder inserts him/herself into a conversation between two parties, impersonates both the parties and gains access to information that the two parties were trying to send to each other.We have avoided the man in the middle attack by which server generates the 6 digit binary value.The user enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit.Hence the intruders will receive only the six series of ten symbols ,but not the original password.

D. HMAC Algorithm

A keyed-hash message authentication code (HMAC) is the type of message authentication code (MAC) that is involved in a cryptographic hash function and a secret cryptographic key. It is used to verify both the data integrity and the authentication of amessage.The cryptographic strength of the HMAC depends upon the size of the secret key used. The most common attack against HMAC is brute force attack to uncover the secret key.A Brute Force Attack is a password cracking method that uses an automated process to try all possible character combinations until password is found. where H is a cryptographic hash function is the secret key is the message to be authenticated, K' is another secret key, derived from original key K (by padding K to the right with extra zeroes to input block size of the hash function, or by hashing K if it is longer than that block size),|| denotes concatenation, denotes exclusive or (XOR),o_pad is the outer padding (0x5c5c5c…5c5c, one-block-long hexadecimal constant),and i_pad is the inner padding (0x363636…3636, one-block-long hexadecimal constant).

$$HMAC(K,m) = H\Big((K' \oplus opad) \,||\, H\big((K' \oplus ipad) \,||\, m\big)\Big)$$

E. Implementation

```
function hmac (key, message) {
if (length(key) > blocksize) {
key = hash(key)     }
if (length(key) < blocksize) {
key = key ‖ [0x00 * (blocksize - length(key))]}
o_key_pad = [0x5c * blocksize] ⊕ key     i_key_pad
=   [0x36 * blocksize] ⊕ key
return hash(o_key_pad ‖ hash(i_key_pad ‖ message))
}
```

VI. FILE SHARING BETWEEN TWO USERS

If any of the users need to view the post e.g. (Video/Image) the request is sent to Server which will look up for the nearby devices. If there are one or more devices in close proximity, the server will check whether the requested file is available with the nearby user. If the content is available with any of the user, server triggers both the nearby devices in back end Service Thread that already running in the mobile devices to start a Bluetooth communication. Here we handled both paired and unpaired devices and this is through pre sharing of Bluetooth ids by server to neighboring devices. After successful Bluetooth initialization the contents will be transferred from source mobile to destination mobile. The privacy of entire user is

retained by having pseudo identities for all the communications.

VII.CONCLUSION

Nowadays, mobile access to social networks has become very popular in many sectors of our society, due to the large amount of personal data and useful information aggregated and made available by applications such as Facebook, Twitter, Google Plus, and so on, that can be viewed as the on-line interfaces of our own lives. However, since such data may contain and/or expose very sensitive information that can be prone to several types of misuses (personal data leakage, identity theft etc.), controlling the access to these facilities through proper authentication procedures is now an essential challenge. The authentication phase is often considered as the weakest element in mobile access security since malware threats are increased that are able to track and capture the secure codes entered by the users.

This work introduced an authentication method (Bright Pass) that prevents malware from being able to compromise mobile access to social network and subverts the user authenticated operations. The proposed scheme uses screen brightness as a secure communication channel to communicate a random sequence which is generated by the secure element to the user. This sequence tells the user when to input correct PIN digits and when to input misleading lie digits. Thus, the user authenticates with a trial for each authentication.

The security analysis shows that the proposed scheme is resilient in opposition to brute force attacks, dictionary attacks, side channel attacks and spyware based recording attacks. From a usability point-of-view, the results of our experiments suggest that the proposed scheme offers a short authentication time and low error rates. Thus, it increases the security while maintaining good usability properties in the social scenario. The comparison with existing schemes that are resilient to multiple recording attacks shows that Bright Pass has similar security strength with considerably lower authentication time and error rates. Therefore, this technology may introduce a positive impact in the social networking environment by changing the associated business dynamics, together with the way of accessing and publishing information on social media, with the obvious consequences in the political and professional sectors that are extremely dependent on such media. Finally, it should be considered that the same mechanism can also be used to secure transactions protected by PIN verification codes in electronic payment application.

VIII. REFERENCES

[1] Aviv, A. J., Sapp, B., Blaze, M., Smith, J. M.: Practicality of accelerometer side channels on smartphones. In ACSAC'12: Proceedings of the 28th Annual Computer Security Applications Conference, pp. 41-50. ACM, New York, NY, USA (2012). Doi: 10.1145/2420950.2420957.

[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] L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum. reCAPTCHA: Human
Based Character Recognition via Web SecurityMeasures. Science, September 2008.

[5] Goodfellow, I.J., Bulatov, Y., Ibarz, J., Arnoud, S., Shet, V.: Multi-digit number recognition from street view imagery using deep convolutional neural networks. ICLR (2014)

[6] Reynaga, G., Chiasson, S. and van Oorschot, P. C.: Exploring the usability of captchas on smartphones: Comparisons and recommendations. In Proceedings of 2015 Network and Distributed System Security (NDSS) Symposium. pp. 8-11, (2015, February).

[7] Chow, R., Golle, P. Jakobsson, M., Wang, X., Wang, L.: Making CAPTCHAs clickable. Ninth Workshop on Mobile Computing Systems and Applications (HotMobile 2008).

[8] J Elson, JR Douceur, J Howell and J Saul. Asirra: a CAPTCHA that exploits interest-aligned manual image categorization. Proceedings of the 14th ACM conference on Computer and communications security (CCS),2007.

[9] M. Shirali-Shahreza and S. Shirali-Shahreza, Drawing CAPTCHA.Proceeding of the 28 international conference on information technology interfaces, Cavtat, Croatia, 2006, pp. 475-480.

[10] Liao, C.J., Yang, C.J., Yang, J.T., Hsu, H.Y. and Liu, J.W. A Game and Accelerometer-based CAPTCHA Scheme for Mobile Learning System.In. Jan Herrington et al. (Eds.), Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2013, pp.1385-1390, (2013).