International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

AUTHENTICATION SYSTEM IN SOCIAL NETWORKS

A.R Preethi[1], M.Gayathri[2], P.Jayasri[3], J.Jenny Sarah[4]

[1]*Assistant Professor, Dept. of Information Technology, Jeppiaar SRR Engineering College, Tamil Nadu*
[2,3,4]*UG Student, Dept. of Information Technology, Jeppiaar SRR Engineering College, Tamil Nadu*

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. Such applications, may involve mobile ticketing, identification, access control operations, etc., are often accessible through social network aggregators. 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, perform unauthorized mobile access to social network services without the user's consent. 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 various types of attacks. We compare BrightPass with existing schemes, in order to show its usability and security within the social network arena. Furthermore, we empirically assess the security of BrightPass through experimentation. Our tests indicate that BrightPass protects the PIN code against automatic submissions carried out by malware while granting fast authentication phases and reduced error rates.*

Key Words: **Authentication, Mobiles, Social networks, Malware attacks, Brightpass scheme**

1. INTRODUCTION

Social networks are one of the most important communication platforms of the last 15 years with high socio-economic value. Social networks are an inherent part of today's internet and used by more than a billion people worldwide. Over the last few years mobile communication devices have becoming powerful and today many of them support application being installed and executed on the device. Mobile devices use sophisticated applications that make life easier and more relax and convenient for users. Because of this people expect these social networking services to be available on their mobile devices. It allows exchange of user-generated content like data, pictures, and videos. Unfortunately, as the importance of these platform rises, the interest of the hackers on them increases well, so that theft of user information and authentication breaches, become problems in social networking area. Many attacks are successful in accessing social networks accounts and the authentication mechanism is not efficient and vulnerable to automated attacks. Many of the top most social networking services providers such as google, facebook, yahoo, twitter, snapchat and dropbox already allow you to optionally require second authentication. Unfortunately, the mobile devices used for gaining access are often vulnerable to several kind of malware. Mobile malware is a malicious software that is specifically built to attack mobile phone or smartphone system. This is kind of malware can be able to retrieve all type of user information such as passwords and PIN codes which are used for perform authentication in social networking applications.Hence,the presence of malware in mobile devices reduces impact on social networks. To overcome malware attack numerous authentication methods are discovered. But those processes are takes long authentication time, having high error rates so they are low acceptance among the users.

In this paper we discuss about BrightPass which enhancing the security and protection it is the simplest effective technique consist of two screen captures when brightness is high have to enter correct pin digit and when brightness is low have to enter the fake one. Compare with existing techniques BrightPass increases user confidence and create great impact on social network access. It provides high security for mobile and sensitive applications against different types of malware attack.

2. RELATED WORK

Nowadays smart phones are built using mobile operating system that allows them to run application with rich and modern functionality. This type of smart phone are designed with new communication interface to carry out security critical operations which can access personal data in application using alpha numeric password. This system leads to spread across online market places and fool the user. This approach helps in preventing the spyware stealing the user credential.

Yi.et.al. proposed a Pass Window which uses PIN digits and pre -selected image called pass icon.

Chow et al. introduce idea of showing special CAPTHCA into a clickable CAPTHCA. These frameworks do not depend on console input the client is requested to choose few component in the network that match the test case.

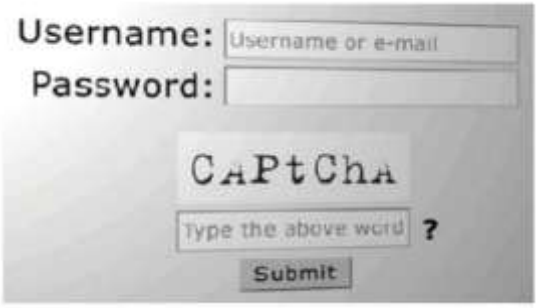

Fig-1: ReCAPTCHA

Fig -2: Clickable CAPTCHA

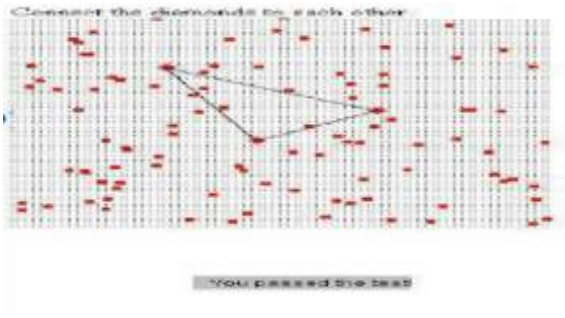

Fig -3: Drawing CAPTCHA

Fig -4: AccCAPTCHA

Kim et al. proposed a Password authentication scheme based on dummy-key called Fake PIN which consists of alpha numeric text and password as a secret value.

Asirra that displays 12 images of butterflies and asks users to select all cat images among them.

Shirali-Shahreza et al. proposed CAPTCHA mechanism for mobile phones called drawing CAPTCHA. In this method dot are displayed on the screen.

Liao et al. proposed a new CAPTCHA scheme based on game logic and human recognition. Here the user as to play a rolling ball game to pass the CAPTCHA challenges.

3. THE BRIGHTPASS CONCEPT

This approach contains a right PIN Number in a 6 digit format which is stored in a larger way. The request of PIN digit position created by SE and further imparted to the client exchanging circle's splendour esteems is high client must enter the right PIN digit whether it looks dim client must enter the deceptive lie PIN digit. This method is used by user and security elements to know the real pin digit with its positions.

3.1 REGISTRATION AND LOGIN

The user creates an account and registers their password to provide user's information such as phone number, e-maid id and location. If someone tries to access your account the server generates four digits PIN number for authenticating user account. The registered mobile no and e-mail id will get alert about your account in some cases

3.2 USER VALIDATION

It is a new PIN-entry method. The basic layout of this method comprises a vertical array of digits from 0 to 9, juxtaposed with another array of ten familiar symbols such as + and / etc. These symbols are moveable in the vertical order using up and down buttons. At first, decide the symbol for the first digit of the PIN. After the first round when the symbol is decided, then in the consecutive rounds enter the second, third & fourth digit of the PIN.

3.3 IMPLEMENTING SCREEN BRIGHTNESS FOR AUTHENTICATION

Spyware attack will be avoided by proposing the idea that uses the screen brightness as an authentication tool. For authentication the server 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 or random PIN number. This proposed work will remove the digits which inserted while the screen brightness is low and takes the digit which is inserted when the screen brightness is high authentication. The server get the signature of user generated PIN and generate the signature value for the Original PIN and compares both the signatures. If the Signatures are equal the user can access their Profile. If not user access their profile.

3.4 SHARING INFORMATION

Social network is an online platform which helps the people to share personal or career information. These social networks are distributed across many platforms

Fig- 8, 9, 10, 11, 12, 13: Screen Captured For All Rounds during Authentication

Fig -8

Fig -9

Fig -10

Fig -11

Fig-12

Fig -13

for linking and organizing people to share knowledge and information. Generally, in social network site people can share their ideas, digital photos, and videos, posts to inform others about real world activities.

4. OVERALL CONCEPT

4.1 PIN-BASED MOBILE AUTHENTICATION METHOD FOR SENSITIVE OPERATIONS.

The PIN-based mechanism to give security to versatile confirmation. For instance, consider a twitter account it's one of the informal organizations. The customer can prepare to get to the record before itself its need to outline the record with the objective that require a minute factor check by adding a phone number to the twitter account profile. When we marked into the twitter account and after enter the passageway mystery word, the customer asked for to enter a six-digit PIN number got by customer enlisted flexible number through text. Once entered the correct PIN number the customer can proficient access the twitter account. In any case, the spyware attempts to get to the portable to get the PIN number and attempt to login this record without the client assertion.

4.2 BRIGHTNESS AS SECURITY MECHANISM

Fig -13: Proposed Authentication Concept

The Bright pass method is one of the screen capture and recording techniques which does not change the screen brightness (SB) setting into the smartphones. Using Bright pass mechanism captured the brightness level which is displayed on the smartphones and compare with visually. The versatile malware tries to get to portable OS and get screen splendour esteem. We utilized the Brightness of brilliant pass application without changing the framework's splendour esteems and store the esteem subtly in the protected components when the client cooperates with the application to enter the PIN. The Bright pass mechanism provides sufficient security against the attacks.

5. SECURITY ANALYSIS

Here we use Bright pass mechanism against shoulder surfing attack, man-in middle attack, Brute force attacks, Dictionary attacks, spyware attack, side channel attack

5.1 SHOULDER SURFING ATTACK

Shoulder surfing attack is one of the immediate perceptions strategies. For example, by using one shoulder to get data. It is used to get secret key, pin, security code of the individual. In Proposed System we use pin passage technique and joystick to select the symbol which is used as password in a secret manner. This will avoid shoulder surfing attack.

5.2 MAN-IN MIDDLE ATTACK

Man-in middle attack is a conversation between 2 parties and both are accessing the Information and send to each others. In Proposed System we can avoid this attack, entering six-digit PIN number by user and server generates six-digit binary number. To prevent information's from main-in middle attacks, Base64 and HMAC algorithms are used. This two algorithms provide encryption and signature values.

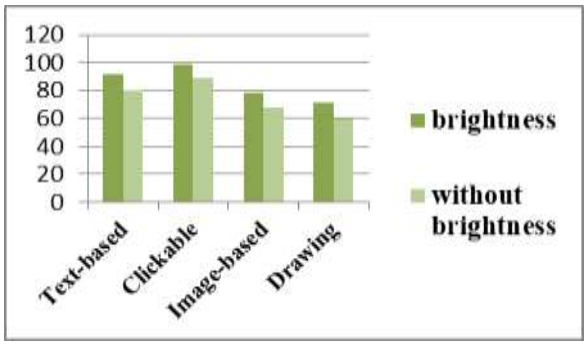

Chart -1: Comparison with Existing System

5.3 BRUTE FORCE AND DICTIONARY ATTACK

Both a brute force attack and dictionary attack are guessing attacks, they are not directly looking for a flaw or bypass. This attack either can be an online attack or offline attack. A Brute force attack is a secret key used to get client watchword. This method contains most of the basic word as secret key and check remaining word with all the possibilities until it get matched. A Dictionary attack is a guessing attack which uses precompiled list of options. Rather than trying every option, only try complete options which are likely to work.

5.4 SIDE CHANNEL ATTACK

This system contains 2 elements to avoid side channel attack. One is the randomization of pin digit for authentication and second one use of screen brightness in secure way. Bright pass mechanism is divided into 2 categories of security

5.5 SPYWARE ATTACK

It is the type of the malware attack install in our system without the knowledge of user. Spyware is used to get the information about the password, credit card, banking credential using internet. Spyware is mostly used to collect the information from the mobile in a secret way. This attack can be avoided by using Bright pass mechanism.

5.6 SMART PHONE THEFT

Even though the smart phones are stolen by someone, it is impossible to access by them with the wrong password. The authentication is provided for all user account by verifying with the help of password. It provides security for all users by preserving and protecting the data from unauthorized person.

6. CONCLUSIONS

In the modern era, the computerized world, including websites, applications, emails, and social networks became a significant part of our life. Due to the vast amount of information users publish on social networks, these platforms both aggregate and display a wealth of valuable information about users and their activity, that can be exploited by various hostile and malicious players.

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 capture by spyware. The security analysis shows that the proposed scheme is resilient against side channel attacks, Shoulder surfing attacks, Man in middle attacks and spyware attacks. From the experimental analysis this BrightPass mechanism offers low error rates in authentication part. Thus this technology creates a positive impact in the social networking environment. Finally, this mechanism can be extended for the secure online transaction protected by PIN verification code.

7. REFERENCES

[1] Meriem Guerar, Mauro Migliardi, Alessio Merio, Mohamed Benmohammed, Francesco Palmieri, and Aniello Castiglione, "Using Screen brightness to improve security in mobile social network access"Member, IEEE Transactions on dependable and secure computing, VOL. 15, NO. 4, JULY/AUGUST 2018

[2] Saranya, R., Gowri, S., Monisha, S., Vigneshwari, S., "An ontological approach for originating data services with hazy semantics", Indian Journal of Science and Technology-0974-5645, Vol 9(23), June 2016/1-6 Scopus

[3] T.Wang, Y.Chen, M.Zhang, Y.Chen, and H.Snoussi, "Internal transfer learning for improving performance in human action recognition for small datasets," IEEE Access, vol.5, pp. 17627-17633.

[4] M. Korakakis, E.Magkos and Ph.Mylonas, "Automated CPATCHA solving: An Empirical Comparison of selected Techniques", 2014 9th International Workshop on semantic and social Media Adaptation and Personalisation. Doi: 10.1109/SMAP.2014.29

[5] D.Pequegnot, L.Cart-lamy, A.Thomas, T.Tigeon, J.Iguchi-cartigny, Jean-Louis Lanet, "A Security Mechanism to Increase Confidence in M-Transaction".

[6] Sandipkumar M Vaniya, B. Bharathi, "Exploring object segmentation methods in visual surveillance for human activity recognition", International Conference on Global Trends in Signal Processing, Information Computing and Communication, pp. 520-525, 2016.

[7] Bandaru R, Albert Mayan J (2016), "Novel approach for whole test suite generation using metamorphic relations", Indian Journal of Science and Technology, Vol 9, No.10, pp.1-7.

[8] Vigneshwari. S and Aramudhan. M (2015), "Personalized cross ontological framework for secured document retrieval in the cloud", National Academy Science Letters-India, Vol. 38 (5), pp. 421–424.

[9] Kalpana, S., Vigneshwari, S, "Selecting multiview point similarity from different methods of similarity measure to perform document comparison", Indian Journal of Science and Technology-0974-5645, Vol 9(10),March 2016/1-6. Scopus.

[10] 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)