ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 2, February 2016

Survey: A Study on Behaviour based Authentication for Mobile devices

Sreeja.P[1], Geethu P.C[2]

PG Scholar, Department of Computer Science and Engineering,
Vidya Academy of Science and Technology
Thrissur, Kerala, India[1]

Asst. Professor, Department of Computer Science and Engineering,
Vidya Academy of Science and Technology
Thrissur, Kerala, India[2]

Abstract: The drastic increase in the use of mobile devices nowadays by people led to a greater increase in need of enhanced security. Many authentication models are available which have been widely used by people all over the world. The problems in the available models and users need for a better level of security lead to the thought of new authentication models in which the key factor is the way people behave. Survey on authentication methods based on behavior is discussed in this paper.

Keywords: Authentication, Security, Behavior, Habit based authentication

I. Introduction

Mobile devices are nowadays in hand of every people you cross by. We use mobile not only for making calls but also for accessing social networking sites, making online payment, credit card transactions.etc. Apart from these, lot of sensitive data is also stored in mobile devices. According to Cisco VNI Global Mobile Data Traffic Forecast, the number of global mobile devices and connections in 2013 has grown to 7 billion, which will exceed the world's population by 2014. [1] According to Mcafee mobile security report, 82 percentage of apps tracks you and 80 percentage is collecting information whenever we use mobile. [11] Authentication process is basically an activity done by the system to verify the identity of the person who is accessing the system. An insecure authentication can damage your privacy. The main three types of authentication models are based on "something you know", "something you have" and "something you are".

Authentication based on "something you know" includes use of username and password, PIN or pattern. Here, the user has to provide a username and corresponding password correctly in order to enter into the mobile system. It is found to be the easiest and cheapest method, but also easiest method to beat. The threat of shoulder surfing, dictionary attack, software cracking, brute force attack exists in this method. [3] Authentication based on "something you have" includes use of some object that must be with you any time you want to be authenticated (eg; Credit card). Authentication based on "something you are" includes use of behavioural and physiological characteristics of a person for authentication. In face recognition, it is difficult to change the pattern as there is only one pattern for an individual and also possible by the attacker to fool the technology by making it believe he/she is the authenticated user by using high resolution photo of the user. [8] The use of fingerprints also have problems. According to an article in CTV news, fingerprint scanning system of apple iphone 5s have been successfully hacked by German students by using the fingerprint of the user photographed from the glass surface and creating a fake finger print that could unlock the device. [10]. The main drawbacks of first two methods lead to the behavioural authentication method which are very much integrated to the normal user's habits and behaviour and proves to be very user friendly. This method can improve security to a higher level giving user an enjoyable experience while authenticating to their own mobile devices.

All Rights Reserved © 2016 IJARTET

The paper is divided into sections. Section 2 describes various behaviour based authentication methods for mobile devices. Section 3 concludes the survey.

II. Behaviour Based Authentication

The security issues in previous discussed biometric methods lead to a new area called behavioural biometrics. Behavioural biometrics deals with not only the physiological characteristics, but also psychological qualities of a person. It is based on what people do and how they do it.

Various behavioural biometric verification methods include keystroke dynamics, gait analysis, voice ID, mouse use characteristics, signature analysis and cognitive biometrics. This feature is found to be unique since it is based on how people do things and different people have different behaviour. This type of authentication is considered as secure since there is no visual input like keyboard and in that case input is hidden. [7] This method is used for secure authentication in financial institutions, businesses, government facilities and retail point of sale (POS), as well as in other environments. Various researches have been done and still going on in this area.

In the research done by Anna Schlenker et al., various behavioural methods are discussed: signature dynamics in which appearance, shape, timing and pressure applied by user while doing signature is measured. It is found to be difficult to be replicated by trained human forger. Voice verification is another method where tone, pitch and cadence of the voice are considered. Mouse dynamics is another method where distance, speed and angle during the mouse movement are measured. Results show that these methods are less obtrusive, does not require special hardware and they are easier and cheaper to use. [2]

In paper [4] proposed by Saevanee, H et al., behavioural manners of user on a touch screen by detecting finger pressure and keystroke dynamics is used. Key press duration and force given by the user while touching on the screen is used here as authentication factor. Here three features are used: duration of interval between two keys, hold time and finger pressure applied while touching on screen. Results show that this method has high accuracy of about 90 percentage and this can assure that system is well protected.

The paper [13] by A. Buchoux et al., based on keystroke analysis proposes a method that combines keystroke analysis with another method can improve the protection. It is a two factor authentication method that combines secret knowledge like 4 digit pin with keystroke analysis. Through utilizing secret-knowledge and keystroke analysis, it proposed a stronger and more robust mechanism. A secret-knowledge based technique will be utilized as usual; however, keystroke analysis will be applied to the input to provide a second verification. Whilst keystroke analysis using mobile devices have been proven effective in experimental studies, these studies have only utilized the mobile device for capturing samples rather than the more computationally challenging task of performing the actual authentication. Given the limited processing capabilities of mobile devices, this study focuses upon deploying keystroke analysis to a mobile device utilizing numerous pattern classifiers.

According to the paper [9] proposed by Markus Jakobsson et al., mobile users can also be authenticated by using those actions that they carry out. A score is calculated based on the actions of the user. It is done by boosting the score when a common habit of the user is identified and degrading the score when activity that is not commonly seen in a user is identified. After a time period, no explicit authentication like password is needed to authenticate. Results show that this approach has great potential while using with devices having rich input.

Another method by Wazir Zada Khan et al., suggests a graphical password based system for mobile devices. This scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. In this, user has to select a username and a textual password. After selecting one of the objects shown, the user has to draw those selected objects on a touch sensitive screen using a stylus. During authentication, the user has to give his username and textual password and then give his graphical password. This method proved to be effective, but it is inconvenient for people who are uneducated and also who have shivering since it is based on drawing compared to other methods. [14]

In paper [12] by Ramanujan Kashi, user’s observed usage of device is compared to an expected pattern of usage. Observed usage can be any daily activity of a person like checking mail, contacting a person, following a route.etc. If any deviation occurs, results in unauthorized access. When this deviation exceeds a threshold, explicit authentication is need. This method proves to user friendly compared to other methods as it is based on their daily activities.

One of the promising factor that can be taken into account in behavioural biometrics is the habit of a person. Habit is routine of behaviour that is repeated regularly and which happens in unconscious layer of mind. Due to this, it is said that it is very difficult to be reproduced. Incorporating such a habit with authentication can enhance security. it will be unique and user friendly. Habits can be whistling to music, tapping a rhythm, making some facial expressions or may be any daily activity that people do.

In paper [7] by JAMIE SETO, the habit that is taken into study is music. Music is something that gives pleasure to mind. Everyone would love to hear music even if they are not a passionate music lover. Tapping rhythm is one of the most seen habits of many people. So this is utilized here by using rhythm of music as an authentication factor. Results show that tapping rhythm on the phone is an effective method since different person interprets rhythm of music differently. The user has to tap rhythm on the phone to authenticate him/her. If the rhythm matches with the one given during registration, authentication completes. Compared to methods discussed earlier, this method has many advantages that make this more promising one.

This method will give user an enjoyable experience during authentication since it is combined with their habits. So it will be very user friendly and very difficult to be reproduced by other person. Unlike biometric method, user can change the rhythm easily whenever needed. User can set complex rhythm according to their mind to make attacker's job difficult. In traditional method, when credential is compromised, whole security of mobile is gone from users hand and attacker can take over the whole control of mobile. But while using rhythm, even if the rhythm is understood by the attacker, it is very much difficult for the user to replicate the tapping motion. Results show that this method is more safe and easy to use in public places as no visual input is there and difficult to be followed by any other person. The chance of shoulder surfing also is less as user can tap at the back of the phone. Accelerometer is the sensor used to capture the user's tapping motion. It measures acceleration, angle of force when user taps. It has gravity component problem, but has no accumulated error. While using accelerometer, actual orientation is not considered and it can cause error during authentication. Recent research shows that gyroscope can be used together with accelerometer so that orientation of the phone also can be taken into consideration and the gravity component problem can be solved. Authentication is done through adaptive learning. Research shows that the best of the learning algorithm that can be used is Fuzzy ARTMAP which performs fast learning of events and can provide better results. This method also enhances security as there is no need of extra hardware and satisfies use-in motion requirements such that user can use this while in motion. [7]

Researches on this have been done by Yimin Chen et al., in which user has to tap on a touch screen rather than at corner or back of the phone. [5] Lot of researches on this area is still going on and there is scope for more extension by incorporating more habits to the authentication and by extending this to web authentication.

III. Conclusion

The development of technology and user security needs require more effective ways of authentication that can beat any attacker. The existing authentication methods proved to be ineffective in providing sufficient security for mobile devices. By incorporating behaviour of people into authentication, various actions of people and how people do that is considered as the important factor for authentication. Incorporating user's habit with authentication can make authentication process an enjoyable experience for the user and more user friendly and secure authentication methods can be evolved.

References

[1]. Cisco. (Feb. 2014). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018.[Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/visual-networking-index-vni/white_paper_c11-520862.pdf

[2]. Anna Schlenker, Milan Šárek, "Behavioural Biometrics for Multi-Factor Authentication in biomedicine", EJBI – Volume 8 (2012), Issue 5.

[3]. A. Sethi, O. Manzoor, and T. Sethi, "User Authentication on Mobile Devices", Cigital, Dulles, VA, USA, 2012.

[4]. Saevanee, H., Bhattarakosol, P.: "Authenticating user using keystroke dynamics and finger pressure". In: Proc. of the Sixth IEEE Conf. on Consumer Communications and Networking. pp. 1078–1079 (2009).

[5]. Y. Chen, J. Sun, R. Zhang, and Y. Zhang. "Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices". InfoCom 2015, Hongkong, China, 2015.

[6]. Ms. K. M. Brindha Shree , Mrs. M. Rajalakshmi, "Biometric Based Secured Authentication in Mobile Web Services", ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013.

[7]. JAMIE SETO, YE WANG, AND XIAODONG LIN, "User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices", IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, VOLUME 3, NO. 1, MARCH 2015.

[8]. Emir Kremi, Abdulhamit Subasi, "The Implementation of Face Security for Authentication implemented on Mobile Phone", http://www.researchgate.net/journal/16833198_International_Arab_Journal_of_information_Technology.

[9]. M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices" in Proc. 4th USENIX Conf. Hot Topics Secur. (HotSec), 2009, pp. 9–15.

[10]. Has the iPhone 5S Fingerprint Scanner Already Been Hacked? [Online]. Available: http://www.ctvnews.ca/sci-tech/has-the-iphone5s-fingerprintscanner-already-been-hacked-1.1468316, accessed Dec. 12, 2014.

[11]. McAfee. (Feb. 2014).Who˝s Watching You? [Online]. Available: http://www.mcafee.com/ca/resources/reports/rpmobilesecurityconsumer-trends.pdf

[12]. Ramanujan Kashi, “Habit based Authentication”, United States Patent Application Publication, US 2009/0049544 A1, Feb. 19, 2009.

[13]. A. Buchoux and N.L. Clarke, “Deployment of Keystroke Analysis on a Smartphone”, Australian Security Management Conference,2008.

[14]. Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, “A Graphical Password Based System for Small Mobile Devices”.

BIOGRAPHY

Sreeja.P is a postgraduate research student at Vidya Academy of Science and Technology, Thrissur, India, affiliated to Calicut University. Her area of interest is security in mobile platforms and new authentication methods. She received her B.tech Degree in Computer Science and Engineering from MG University, Kerala, India, in 2013.

Geethu P.C is an Assistant Professor at Vidya Academy of Science and Technology, Thrissur, India, affiliated to Calicut University. Her area of interest is Network Security. She received her M.tech Degree in Computer Science and Engineering from Kerala University, Kerala, India, in 2013.