International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

Obtrusive and Unobtrusive Authentication of Portable Devices for Security

Jyoti R. Rana

Designation : Assistant Professor
Affiliation : Naran Lala College Of Professional and Applied Sciences
Email : jyotirrana@gmail.com

ABSTRACT

In this information edge, everyone carry one or more portable devices with them. As far as security of these devices is concerned, no specific method is found yet that only provide security of these devices. This paper focuses on various methods for authentication of these devices. Portable devices can be authenticated by two ways: Implicit authentication which does not require user attention such as Gait authentication and explicit authentication which require user input such as finger print recognitiion, speech recognition, iris matching, PIN & password based authentication etc.

Keywords:

Biometrics; Obtrusive; unobtrusive

INTRODUCTION

In this computing edge, portable devices are used widely as a communication tool. Moreover these devices contain large amount of personal information as well as sensitive data, because these devices are not only used as communication tool but also to access various services such as net-banking, etc. Therefore lot of risk is associated with these devices. Traditionally user of a portable devices are protected by providing them PIN codes and passwords. This is not enough to protect these devices and data available in these devices in normal scenario. Many mobile phone users consider the PIN to be inconvenient as a password that is complicated enough, easily forgotten and noticeable by anyone[1]. Very few users change their PIN regularly for higher security. So there is a need of developing method which uses person's behavioral characteristics which are not noticeable by anyone as well as require less attention of user. Biometrics systems use persons' behavioral characteristics and they provide very high level of security as they are not forgotten by user just as passwords and PINs. Biometrics use fingerprints, voice, face, iris, gait and signature and works with specialized sensor devices such as camera, acceleration sensor, today's portable devices with their unique features such as small size, low cost, functional sensing platforms, computing power, its wireless communication capability, is opening up new areas in biometrics that hold potentials for security of mobile phones, remote wireless services and also health care technology. To provide resilient security to these devices, biometrics can be used with these devices which facilitate trustworthy electronic methods to access various services via these portable devices.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

REVIEW OF LITERATURE

Computing has become prevalent in almost all aspects of human endeavor. With dawning of information age, need as well as demand of mobile and portable devices is increasing in medicine, law, management and education. This enables to use such devices not only as communication tools but also in an application like m-banking or m-government [2-3]. This means that they can store and process valuable information such as financial or private data. This also increases the risk of being target of attacks. According to UK statistics in every three minutes a mobile phone is stolen [4]. The current protection mechanisms of these devices are usually based on PIN codes or passwords. Nowadays a normal user has on average 21 passwords to remember [5]. Unfortunately, 81% of the users select common words as a password and 30% of users write their passwords down, which equally compromises security [5]. While offering a large amount of applications, most mobile devices only offer one kind of authentication method which is knowledge-based (e.g. PIN or password). As studies have shown, these methods are not well accepted by the users [6]. A survey shows that 66% of the respondents use PIN authentication only at switch on and only 18% of the user also utilize the standby mode authentication [1].

With the property of S.S.O (Single Sign-on) a user logs in once and gains access to all systems without being prompted to log in again at each of them. Therefore, SSO does not defend against theft and compromise of devices well, and does not address voluntary account sharing at all. So that users want a solution to authentication that increases security, provides transparent authentication and "authenticates the user periodically throughout the day in order to maintain confidence in the identity of the user" [7]. Different biometric characteristics such as fingerprints [8] already have been proposed to improve security of mobile devices. Biometric characteristics have the advantage that, unlike passwords, PINs, tokens etc., they cannot be stolen or forgotten. The main advantage of biometric authentication is that it establishes an explicit link to the subject's identity because biometrics uses human physiological and behavioral characteristics. However, both fingerprints and password entry are obtrusive and require explicit action from the user, which is not convenient in a frequent use. In order to improve security in mobile and portable devices, an unobtrusive mechanism of authentication is desirable.

For finger print based identification on mobile phone, Chen et al. have investigated that fingerprint recognition needs external hardware as well as algorithm for internal hardware for recognition purpose[9]. In [10] Daugman reported that the original iris patterns are randomly generated after almost three months of birth and are not changed all life. So he puts forward his study to identify a person using unique iris patterns. According to him, iris of any normal human being contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collaret [11]. Major challenge of Iris biometric is the iris image quality as bad image quality will affect entire iris recognition process. So further, they integrated the use of digital cameras for acquiring images at high resolution. So that

image processing task can perform on the phone itself. In [12] Chen & Huang developed a biometric for voice. According to them, a voice signal conveys a person's physiological characteristics such as the vocal chords, glottis, and vocal tract dimensions. Automatic speaker recognition (ASR) is a biometric method that encompasses verification and identification through voice signal processing. The speech features encompass high-level and low level parts. While the high-level features are related to dialect, speaker style and emotion state that are not always adopted due to difficulty of extraction, the low-level features are related to spectrum, which are easy to be extracted and are always applied to ASR. One major challenge of ASR is its processing cost. All this biometric identification requires attention of user. So they are useless without user input. It leads requirement of identification method which is by nature unobtrusive, privacy preserving and controlled by the user, who would not at all be disturbed or burdened while using this technology. So without user intervention, device should be verified. In [13] Woodward et. al., have introduced a new biometric method based on walking manner of person i.e. Gait. He stated that Gait of a person is a distinctive characteristic for individuals. Gait recognition has been studied as a behavioral biometric for more than a decade, utilized either in an identification setting or in an authentication setting. Early studies from psychology [14], medicine [15] and biometrics [16], [17] already give evidence that human gait contains very distinctive patterns as well as unobtrusive mechanism that can be used for identification and verification purposes. In [18] Bours & Shrestha stated that traditionally 3 major approaches have been developed for gait recognition referred to as the Machine Vision (MV) based gait recognition, in which case the walking behavior is captured on video and video processing techniques are used for analysis, the Floor Sensor (FS) based gait recognition by placing sensors in the floor that can measure force and using this information for analysis and Wearable Sensor (WS) based gait recognition, in which scenario the user wears a device that measures the way of walking and recognize the pattern recognition for recognition purposes. In [19]Tanviruzzaman et al., investigated that Smart phone, such as an iPhone, is now incorporated with accelerometers working along three primary axes, which could be utilized for gait recognition to identify the user of a mobile phone. Mobile phone based biometrics uses the acceleration signal characteristics produced by walking for verifying the identity of the users of a mobile phone while they walk with it. In this situation, the three-dimensional movement produced by walking is recorded with the accelerometers within a mobile phone worn by the user. Chang et al. [20] used accelerometers in television remote controls to identify individuals. Kale et al. [22] and Gafurov et al. [21] used gait recognition to detect whether a device is being used by the owner. Most of the previous works in gait recognition are based on machine vision techniques i.e they process video or sequence of images to extract gait patterns. We will refer this type of gait recognition as vision based. Recently a new direction in biometric gait recognition has emerged [22], [23], [24]. Instead of camera, a physical device is attached to the body for collecting gait patterns. Nowadays every

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

mobile and portable device contains built-in accelerometer to record gait pattern. So there is no need of attaching extra hardware in order to collect gait pattern. Accelerometer-based gait recognition was first proposed by Ailisto et al. [25] and further developed by Gafurov [26]. They used high-quality dedicated accelerometers which were placed on the hip, arm or ankle to record the acceleration while the subjects were walking. Only recently researchers started to use mobile devices to record the accelerometer data [27-30].

Feasible scenario of biometrics on mobile phone

Biometric system operates in two modes: identification mode and authentication mode. Identification mode recognizes an individual by searching sample of all users in database for matching. So this mode performs one to many comparisons. Authentication mode validates a person's identity by comparing captured data with his/her own biometric enrolled in database. So this mode performs one to one comparison. Thus at very first stage biometric operates in Authentication mode and then it operates with identification mode.

Algorithm for Biometrics Identification

Step1: Input user's personal Information such as name, age etc. as well as Account information such as email address, password etc.

Step 2: Let device operate in authentication mode so that it can collect templates for verification.

Step 3: Let device operate in identification mode so that user verifies person's identity continuously.

Step 4: In continuous verification,
If match found
Then the device work as usual
And if match not found
Prompt user for other type of verification such as PIN, Password

Step 5: If match not found in Step 4
Then Stop working of device until user enter correct PIN or Password

Step 6: Repeat step 4 continuously

Obtrusive versus unobtrusive

Obtrusive	Unobtrusive
It is noticeable by other persons because users have to give their input and require user attention.	It is not noticeable by other persons because users input is not required and it is performed implicitly
Example include PIN, Password, Pattern matching, iris matching	Examples include Gait recognition etc.
This method is not secure because anyone can notice it.	This method is secure because it extracts person's behavioral characteristics.

Conclusion

To protect portable devices in normal scenario, biometrics deal with high security because it deals with person's behavioral as well as characteristics. So in this paper we discuss all the possible methods for obtrusive as well as unobtrusive authentication by using biometrics of a person's. This paper also discusses

scenario, algorithm and comparison of these two methods for biometrics authentication.

References

[1] N. Clarke and S. Furnell, "Authentication of users on mobile telephones - a survey of attitudes and practices," Computers & Security, vol. 24, no. 7, pp. 519 – 527, 2005.

[2] K. Pousttchi and M. Schurig, "Assessment of today's mobile banking applications from the view of customer requirements." in 37th Annual Hawaii International Conference on System Sciences (HICSS'04), 2004.

[3] Y. Kim, J. Yoon, S. Park, and J. Han, "Architecture for implementing the mobile government services in Korea," in First International Workshop on Digital Government: Systems and Technologies (DGOV 2004), Shanghai, China, November 2004.

[4] "Huge surge in mobile phone thefts," http://news.bbc.co.uk/1/hi/uk/1748258.stm, Last visit: 04.09.2006.

[5] "2002 NTA Monitor password survey," http://www.outlaw.com/page-3193, Last visit: 04.09.2006.

[6] F. Breitinger and C. Nickel, "User Survey on Phone Security," in BIOSIG 2010 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 2010.

[7] S. Furnell, N. Clarke, and S. Karatzouni. Beyond the pin: Enhancing user authentication for mobile devices. *Computer Fraudand Security*, 2008.

[8] "Fingerprint solution to secure mobile phones,"http://www.geekzone.co.nz/content.asp?contentid=1145, [Online; accessed 07-May-2010].

[9] Chen X.; Tian J.; Su, Q.; Yang, X. & Wang, F.(2005). A secured Mobile Phone Based on Embedded Fingerprint Recognition Systems. In: *Intelligence and security informatics*

[10] Daugman, J. (2003). The Importance of Being Random: Statistical Principles of Iris Recognition. Pattern Recognition, Vol. 36, No. 2, (February 2003), pp. 279-291.

[11] Daugman, J. (2004). How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, (January 2004), pp. 21-30.

[12] W. Chen & J. Huang. Speaker Recognition Using Spectral Dimmension Features. Proceedings of 4th international Multi-Conference on computing in the Global information Technology.

[13] Woodward, J. & Orlans, N. (2003). Esoteric Biometrics, In: Biometrics: Identity Assurance in the Information Age, Gatune, J., (Ed.), pp. 115-136, McGraw-Hill Professional Publishing, ISBN 0-07-222227-1, Berkeley, California, USA

[14] H. W. Reese and D. Rodeheaver, "Age-related declinces in motor control," in Handbook of the Psychology of Aging, 5th ed., C. J. Ketcharn and G. E. Stelmach, Eds., USA, 2001, pp. 333–335.

[15] A. A. Kale, "Algorithms for gait-based human identification from a monocular video sequence," Ph.D. dissertation, College Park, MD, USA, 2003, chair-Chellappa, Rama.

[16] D. Gafurov, "Performance and security analysis of gait-based user authentication,"

Ph.D. dissertation, Faculty of Mathematics and Natural Sciences, University of Oslo, 2008.

[17] J. M¨antyj¨arvi, M. Lindholm, E. Vildjiounaite, S.-M.M¨akel¨a, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05), vol. 2, pp. ii/973 – ii/976, 2005.

[20] K. Chang, J. Hightower, and B. Kveton.Inferring identity using accelerometers in television remote controls.In *Proceedings ofthe International Conference on Pervasive Computing*, 2009.

[21] D. Gafurov, K. Helkala, and T. Søndrol. Biometric gait authentication using accelerometer sensor.*JCP*, 1(7):51–59, 2006.

[22] A. A. Kale, N. Cuntoor, and V. Kr¨uger.Gait-based recognition of humans using continuous hmms. In *FGR '02: Proceedings ofthe Fifth IEEE International Conference on Automatic Face andGesture Recognition*, 2002.

[23] R. Greenstadt and J. Beal.Cognitive security for personal devices.In *The First ACM Workshop on AISec*, 2008.

[24] M. Jakobsson and A. Juels.Server-side detection of malware infection.In *NSPW*, 2009.

[25] H. J. Ailisto, M. Lindholm, J. M¨antyj¨arvi, E. Vildjiounaite, and S.-M.M¨akel¨a, "Identifying people from gait pattern with accelerometers," Biometric Technology for Human Identification II, vol. 5779, no. 1, pp. 7–14, 2005, vTT Electronics, Finland.

[26] D. Gafurov, "Performance and security analysis of gait-based user authentication," Ph.D. dissertation, Faculty of Mathematics and Natural Sciences, University of Oslo, 2008.

[27] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition," in Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010.

[28] J. Frank, S. Mannor, and D. Precup, "Activity and gait recognition with time-delay embeddings," in AAAI Conference on Artificial Intelligence, 2010.

[29] J. Kwapisz, G. Weiss, and S. Moore, "Cell phone-based biometric identification," in Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, 2010, pp. 1 –7.

[30] S. Sprager, "A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine," in Sensors, Signals, Visualization, Imaging, Simulation and Materials, 2009, pp. 94–99.