ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

A COMPARATIVE STUDY OF BIOMETRIC VERIFICATION SCHEMES

Karan Madan, Surya World Institute of Engineering & Technology, Bapror

Abstract

The introduction of smartphones, such as those based on Apple, Android operating environment, Microsoft and Blackberry technologies, is rapidly shifting the nature of interactive computing. Much of this is aggravated by the swarm of digital sensors embedded within these equipments, including GPS, touch screens, cameras and microphones etc. As a result, world's expectations around utility of cell phone equipments are changing. Simple gestures i.e. Android screen lock pattern, graphic based passwords and biometric verification are finding its way as alternative cell phone verification mechanisms, but the basics remains the same as passwords and PINs remain the most common schemes used till now. All other schemes may be biometric or non-biometric can be combined with the basic passwords or PIN numbers etc. Each biometric scheme has unique strengths and weaknesses, and has the potential to improve on the Password approach. There are basically three types of biometric schemes. Voice, face and gestures. This study demonstrates practical advantage for Face, and a lesser advantage for Voice in supporting memory task routine.

Introduction

In this paper, we look at verification techniques on cell phone equipments from the end-users' perspective. We study three biometric verification schemes - voice, face and gesture, and combinations of voice with face and gesture.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

A distinctive 8-character password condition is incorporated as a baseline. We measure the time to type an 8-character combined -case alphanumeric password on PC and cell phone phones. On cell phone equipments with soft keyboards, entry of compliant passwords often necessitate the end-user to switch between various keyboard layouts. They discovered that while participants typed the password at the rate of 17 wpm on a PC, they only attain a mean of 6 wpm on their own cell phones.

Even in PC, end-users often choose poor quality passwords. The apparent effort of entering passwords on cell phone equipments will persuade further password simplification, for example insertion of non-alphabetic characters only at the beginning or end of the password. Recollect aids such as writing down passwords and physically affixing them to equipments [1] set additional security risks for password verification in a cell phone context.

Related Work

Community is now adapted to talking into small cell phone equipments, and seeing themselves through the equipment camera. As the superiority of sensors and processing power of cell phone equipments improves, cell phone biometric verification has turn out to be a realistic proposition.

Researchers have also explored union of multiple biometric schemes to compensate for loss of quality in one modality [2][3][4]. For example, Hazen et. al [5] examined the combination of face and voice recognition on an iPAQ equipment, finding noteworthy improvements in recognition accurateness compared to either biometric alone. Krawczyk and Jain [6] examined signature and voice forms on a tablet equipment.

End-user attitudes have been discovered [7][8][9], but relatively slight attention has been given to pragmatic comparison of the usability of various biometric verification schemes.

Toledano et. al's usability assessment of multimodal (non-cell phone) biometric

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

verification systems [10] is a prominent exception. It recommends a examination framework for biometric usability investigation that uses ISO usability aspects (i.e., effectiveness, usability efficiency and satisfaction) for assessment.

Cell phone Biometric Verification

Different usage environments, including deprived lighting, motion/vibration, and ambient sort of noise, pose noteworthy challenges to biometric recognition algorithms. Research has discovered algorithms suitable for use on cell phone equipments [11][12], and for processing face as well as voice data collected in noisy cell phone environments [13], or with very low resolution cameras [14].We suppose that the era of using biometric verification for cell phone equipments is imminent.

All of these investigations focused on recognition performance. Uniting biometrics also supports 'liveness examining' – the ability to discriminate a live end-user from a spoof. Work in this [15] have focused both on biometric analysis and custom end-end-user challenges.

Little is known about the usability of these schemes in comparison to each other, as well as to passwords. Moreover, little is known about the ease with which end-users can simultaneously offer two biometric samples, to encourage efficient multi-factor verification. Biometric verification is a well-studied field of research. Physical biometrics, like face, voice and signature, are the most commonly usable forms. Biometrics verification systems have been evaluated against a rich set of metrics that contain both performance and usability features [16].

Usability Study

All voice and gesture forms used the same verification phrase, '13571357', providing a memorable consistent value crosswise both forms, and an audio sample long enough to be satisfactory for an automated speaker verification technology.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

A repetitive 4-digit sequence was bring into play to increase memorability while still making use of a variety of gestures and also speech sounds. Password entry was incorporated as a reference point.

Three totally different forms of end-user action for biometric verification, password entry, and two combinations were observed in six experimental conditions described below. This paper uses the words 'end-user action' and 'taking action' to refer to the actions taken by the end-user in offering an verification sample (biometric or password).

As verification algorithms improve, these end-user actions will be an vital determinant of technology acceptance. This study assumes a absolutely zero false rejection rate (FRR), that is the ideal scenario for a legitimate end-user. The six testing conditions are given below.

1. Password: Due to typical corporate password policies, the easy to remember 8-character password security was used commonly.

2. Voice: The end-user must speak the password phrase " one three five seven one three five seven" in his own voice that will be totally different and unique from other's voice

3. Face: The end-user must take a photograph of their face using the front-facing photographic device.

4. Gesture: The end-user must write '13571357' on the screen with their finger or by some other means. Gesture input can be of many other forms

5. Face+Voice: The end-user must say " one three five seven one three five seven " while at the same time time lining up their face and taking a photograph by some camera. So combination of two biometric techniques are used.

6. Gesture+Voice: The end-user must say "one three five seven one three five seven"while at the same time writing the digits '13571357' on the screen with their finger.

Conclusion

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

Gain access to business data from cell phone equipments requires secure verification, but traditional password schemes based on a blend of alpha-numeric and symbols are burdensome and detested, leading end-users diminished interest to access business data on their personal equipments. Face and voice biometrics schemes were faster than password entry or any other verification. Speaking a PIN was the fastest among biometric sample entry, but short-term memory recollect was better in the face verification condition as no need to remember anything. The huge set of input sensors on cell phone equipments, including cameras, microphones, touch screens, and GPS, facilitate sophisticated multi-media interactions. Biometric verification schemes using these sensors could suggest a alternative to password schemes, since the sensors are familiar and already used for a variety of cell phone tasks. The study examined basically four points. 1. The time taken to supply an verification sample may be in the form of password, biometric, or combination of any two biometrics 2. Error rates in supplying an verification sample of appropriate quality 3. The impact of the end-user actions on performance in a memory recall assignment 4. End-user reactions to the verification schemes. We find that speaking was the fastest biometric verification scheme, but taking a photograph supported better performance in the memory recall task.

REFERENCES

[1] B. Tognazzini. Design for usability. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People can Use. O'Reilly Books, 2005.

[2] G. Aggarwal, N. K. Ratha, R. M. Bolle, and R. Chellappa. Multi-biometric cohort analysis for biometric fusion. In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Las Vegas, NV, 2008.

[3] J. Basak, K. Kate, V. Tyagi, and N. Ratha. QPLC : A novel multimodal biometric score fusion method. CVPR Workshop on Biometrics, 2010.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

[4] V. Tyagi and N. Ratha. Biometrics score fusion through discriminative training. CVPR Workshop on Biometrics, 2011.

[5] T. J. Hazen, E. Weinstein, B. Heisele, A. Park, and J. Ming. Multimodal face and speaker identification for mobile devices. In R. I. Hammoud, B. R. Abidi, and M. A. Abidi, editors, Face Biometrics for Personal Identification: Multi-Sensory Multi-Modal Systems. Springer, 2007.

[6] S. Krawczyk and A. K. Jain. Securing electronic medical records using biometric authentication. In Proceedings of the 5 International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), Hilton Rye Town, NY, 2005.

[7] N. Gunson, D. Marshall, F. McInnes, and M. Jack. Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits. Interacting with Computers, 23(1):57–69, Jan. 2011.

[8] L. A. Jones, A. I. Ant´on, and J. B. Earp. Towards understanding user perceptions of authentication technologies. In Proceedings of the ACM Workshop on Privacy in Electronic Society, Alexandria, VA, 2007.

[9] R. Tassabehji and M. A. Kamala. Improving e-banking security with biometrics: modelling user attitudes and acceptance. In Proceedings of the 3rd International Conference on New Technologies, Mobility and Security (NTMS), Cairo, Egypt, 2009.

[10] D. T. Toledano, R. Fern´andez Pozo, A. Hern´andez Trapote, and L. Hern´andez G´omez. Usability evaluation of multi-modal biometric verification systems. Interacting with Computers, 18(5):1101–1122, Sept. 2006.

[11] Y. Ijiri, M. Sakuragi, and S. Lao. Security management for mobile devices by face recognition. In Proceedings of the 7th International Conference on Mobile Data Management (MDM), Nara, Japan, 2006.

[12] S. Kurkovsky, T. Carpenter, and C. MacDonald. Experiments with simple iris recognition for mobile phones. In

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M11-052013
VOLUME 3 ISSUE 3 May 2013

Proceedings of the 2010 Seventh International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, 2010.

[13] Adobe Systems Inc. PhoneGap. http://phonegap.com.

[14] Q. Tao and R. N. J. Veldhuis. Biometric authentication for a mobile personal device. In Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose, CA, July 2006.

[15] S. A. Schuckers, R. Derakhshani, S. Parthasardhi, and L. A. Hornak. Liveness detection in biometric devices. In Electrical Engineering Handbook, 3rd edition. CRC Press, 2006.

[16] L. Coventry. Usable biometrics. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People can Use. O'Reilly Books, 2005.

[17] J. G. Trafton and C. M. Monk. Task interruptions. In D. A. Boehm-Davis, editor, Reviews of Human Factors and Ergonomics. 2008.