Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Improving User Authentication with Fingerprint Biometrics and Biometric Personal Identification Number (BIO-PINTM) as a Multi-Factor Authentication Mechanism

Robert Batie Jr.
Nova Southeastern University

Yair Levy
Nova Southeastern University

Steven Furnell
Plymouth University

Peixiang Liu
Nova Southeastern University

Improving User Authentication with Fingerprint Biometrics and Biometric Personal Identification Number (BIO-PIN™) as a Multi-Factor Authentication Mechanism

Research-in-Progress

Robert B. Batie Jr.
Graduate School of Engineering and Computing, Nova Southeastern University, Ft. Lauderdale, FL USA

Yair Levy
Graduate School of Engineering and Computing, Nova Southeastern University, Ft. Lauderdale, FL USA

Steven S. Furnell
School of Computing, Electronics and Mathematics, Plymouth University, Plymouth, Devon, UK

Peixiang Liu
Graduate School of Engineering and Computing, Nova Southeastern University, Ft. Lauderdale, FL USA

ABSTRACT

Previous authentication methods of establishing ones' identity to a computer system, by using a password or presenting a token are vulnerable to circumvention by misplacement or unauthorized sharing. Biometric authentication methods offer uniqueness and permanent human physiological characteristics that are difficult to share or compromise. This study seeks to provide insight into the area of biometric as 'something the user knows,' and 'something the user is.' This concept is where the user presents multiple instances of a biometric (BIO) feature in a sequence, as one would enter a Personal Identification Number (PIN). The user authenticates to the system by presenting fingerprints, finger segments, facial recognition, or other mixture of biometric measures in a specific sequence is being called the BIO-PIN™.

The main goal of the study is to examine the role of three authentication methods

(username/password, BIO-PIN™, & BIO+PIN), and time, on the effectiveness of authentication, as well as the users' ability to remember the BIO-PIN™ sequence, versus username/password or BIO+PIN (multiple fingerprints without sequence & a numerical PIN). Additionally, this research-in-progress (week nine of a 10-week period) examines the authentication methods when controlled for age, gender, user's computers experience, and number of accounts. Preliminary results are presented here. The latest results will be presented along with open discussions on how innovative user authentication method can lead to additional studies.

Keywords: Biometrics, Authentication, BIO-PIN^{TM}, BIO+PIN, Passwords, Personal Identification Number, Vulnerability, Two-factor Authentication

INTRODUCTION

Much attention has been given to the problem of user authentication on the Internet and Web-based applications, including physical or logical access (Woodard and Flynn 2005). Previous methods of establishing ones' identity by using a password, presenting a token, or identification (ID) card are vulnerable to circumvention by misplacement or unauthorized sharing. One of the advantages biometric authentication methods offer over other methods, such as username and passwords or tokens, is that fingerprints and other biometric modalities are unique, and permanent human physiological characteristics that cannot be easily shared or compromised (Furnell, Dowland, Illingworth and Reynolds 2000; Maty´aˇs and ˇ R´ıha 2010).

Traditional user authentication methods, such as username/passwords, still pose a significant vulnerability when accessing information systems (Biddle, Chiasson and Van Oorschot 2012; Furnell 2007). Users are having trouble remembering passwords and may be frustrated with the complex password requirements. User knowledge of creating adequate

passwords (training), the complexity and makeup of the password, and the process for resetting the passwords varies across organizations. Username and passwords are still very cheap to implement because all operating systems have that capability. The problem has become more acute as Internet use grows and fraudulent strategies are launched in an effort to exploit the lack of adequate Internet authentication (Shenk 2007).

Authentication is defined as a way to establish, verify, and prove the validity of a claimed identity of a user, process, or system (Levy, Ramim, Furnell and Clarke 2011). Authentication is usually done by employing one or more of the following methods of (1) providing something the user knows (e.g., password or PIN), (2) providing something the user has (a token, fob, or card), and/or (3) providing something the user is (fingerprint, face, voice recognition, or other biometric attributes) (Hermann 2002; Hisham, Harin and Sabah 2010; Ren and Wu 2012 p. 714).

Biometrics offers a natural and reliable solution to certain aspects of authentication using inherent physical attributes (Ross 2007). Biometrics is the science of establishing identity by using physiological features, characteristics, and traits such as fingerprints, retina venial patterns, irises, voice, face patterns, as well as hand/finger measurements, for identification and authentication purposes (Ross 2007). Web-based services such as e-banking, e-commerce, e-government, electronic medical records, e-learning, and the decentralized services for processing credit card transactions have further enhanced the need for reliable identity/authentication management systems (Ross, Nandakumar and Jain 2006). Thus, the main goal of this research study is to examine the role of the authentication method (BIO-PIN™, & username/password), and time, on the effectiveness of authentication, as well as the users' ability to remember the BIO-PIN™, versus username/password. Moreover, this study compares the BIO-PIN™, with a traditional multi-factor biometric authentication using multiple fingerprints (without sequence)

and a numerical PIN sequence (BIO+PIN). Additionally, since prior studies related to the effectiveness of authentication demonstrated some differences of the results based on age, gender, user's computers experience, and number of accounts, this research study also examines the authentication methods when controlled for the aforementioned four demographics variables.

LITERATURE BACKGROUND

Authentication is defined as the act of confirming that the communicating entity (user, process, or system) is the one claimed (Hermann 2002; Ren and Wu 2012). The need for reliable user authentication techniques has increased due to heightened concerns about security and rapid advancements in networking, communication, and mobility (Jain, Ross and Pantkanti 2006). Biometric modalities such as fingerprints and handprints have long been used as biometric identifiers. Other research efforts have done extensive work establishing an identity using biometric such as feature mosaicking, feature level fusion, multi-biometric systems, as well as two-dimensional (2-D) measurements of the fingers and hand (Jain et al. 2006; Ross, 2007; Woodard and Flynn 2005). Fingerprints and other biometric modalities are unique, and permanent human physiological characteristics that are not easily compromised (Furnell, Dowland, Illingworth and Reynolds 2000; Maty´aˇs and ˇ R´ıha 2010). Multi-biometric is defined as a system that consolidates the evidence presented by multiple biometric sources presented to the mechanism by the same person (Ross 2007; Ross et al. 2006). Multi-biometrics is considered more reliable than uni-biometric systems because it uses multiple pieces of information fused together the results into a single final authentication decision.

Industry standard complex passwords consist of a combination of eight or more characters that include uppercase letters, lowercase letters, numbers, and special characters (Dhamija and Dusseault 2008). Many users today are burdened with managing an increasing

number of authentication requirements, causing password fatigue (Dhamija and Dusseault 2008). It is estimated that users can access as many as 15 accounts with username and passwords on a daily basis. These users typically can only remember four to five different and complex passwords effectively (Gouda, Lie, Leung and Alam 2007). Some users feel they are overwhelmed by the increasing number of usernames and unique complex passwords they are required to use (Dhamija and Dusseault 2008). Passwords can be guessed by running a simple brute force or dictionary attack. Users with multiple passwords tend to write them down, use the same password or a slight variation of the same password for multiple accounts (Forget and Biddle 2008; Hisham et al. 2010). Information systems are vulnerable to compromise as identity theft has become one of the fastest growing crimes on the Internet, leading to significant financial losses and privacy concerns due to of rising online fraud or attacks (Gajek, Löhr, Sadeghi, Winandy and Görtz 2009; Solove 2008). With the significant increases of cyber security breaches, additional investigation into different approaches to improve user authentication appears to be warranted both when accessing systems physically or via the Internet (Mirante and Cappos 2013).

METHODOLOGY

The methodology used in this research study is an experimental multiple baseline design method to evaluate the effectiveness of the BIO-PIN™ authentication method proposed. We are evaluating the role of the *authentication method* (BIO-PIN™, BIO+PIN, & username/password) and *time* on the effectiveness of authentication and users' *ability to remember* the BIO-PIN™ sequence vs. BIO+PIN vs. username/password when controlled for *age, gender, volume of user accounts, or frequency of IT usage*?" The aim of this study is to assess the effectiveness of the user BIO-PIN™ authentication method that uses unique identifying features and the sequence

entered, in an effort to see if users can remember the BIO-PIN™ sequence, compared with an industry standard complex password, and the BIO+PIN method.

Additionally, in this research we are attempting to measure whether there are any significant differences in remembering an industry standard complex username/password, BIO-PIN™ or BIO+PIN over time at intervals of two (2) weeks for a total of 10-weeks. Moreover, we are measuring such differences when controlled for age, gender, number of computer/Internet accounts or frequency of IT use. Prior literature indicated that differences might exist in users remembering passwords based on such demographics indicators. In this experiment, the users are engaged in the treatment for a longer duration, a 10-week period (Levy and Ellis 2011).

In this study all users are asked to remember the authentication methods for the same length of time as a control method. Real-world users may access systems at any time. Some authentications are only used monthly to pay bills online or access a bank account. These systems may offer the option of having the password remembered for you as an option. Creating new passwords may come with the suggested twelve to fifteen character passwords. Some examples of computer-generated passwords are: Bxn D5x JKr cYo; 37T Jf5 uZB Q6T; Yre Pa& Dmb Ca2 tSe; and Rh4 tA0 wSa E&h r#b.

When using computer or web-based password generators, one must have a Password managers or some method to manage complex and randomly generated passwords because they are difficult to remember. Password managers are in essence, a token that can be stolen, lost, corrupted or compromised. The BIO-PIN™ presents an alternative to the authentication problem.

The study used Multivariate Analysis of Variance (MANOVA) statistical method to compare the BIO-PIN™ vs. BIO+PIN vs. Username/Password authentication methods on the effectiveness of authentication, and the role of time on the user's ability to remember PIN vs.

username/password. The Multivariate Analysis of Covariance (MANCOVA) will be used to test the aforementioned differences when controlled by age, gender, user experience, and number of accounts.

The study used a Quota Sampling strategy (50 participants) that ensures to some degree, all the population in the strata is represented. MANOVA sampling recommends a sample size of 100 participants. However, 97 potential candidates were solicited to participate of which 48 agreed. The problem with this strategy is that the degree of generalizability may be questionable (Salkind, 2009). Sample size is noted in the research paper as a limitation.

BIO-PIN™ Application

The BIO-PIN™ application was developed using the Digital Persona® Software Development Kit (SDK). A fingerprint reader, the Eikon II single swipe, is being used to capture the fingerprints. Figure 1 shows the representation of fingertips and a picture of the swipe fingerprint reader used in the study. The BIO-PIN™ application resides on a MacBook Pro that is partitioned to use the Windows 7 operating system in a standalone mode. This application is in the development stage being used strictly for evaluation of BIO-PIN™ concept. It has not been reduced to practice, as the application has not been sufficiently tested.

Users register by selecting a username from one of the names of the 50 United States, 50 state capitals or major cities within the 50 states. When the selected username is less than eight characters additional numbers or alphabets are added to make up the difference (i.e., utah0815, Topeka11, albanyny or Maryland). Next, the user creates an industry standard, complex password of eight or more characters consisting of at least one capitol letter, one number, and one special character and validates the password.

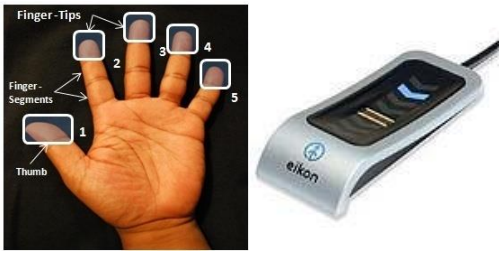

Figure 1. Fingers with BIO-PIN™ and fingerprint reader

User Authentication Process

Then, all five fingerprints from one of the user's hands are presented to the fingerprint reader several times until an acceptable image of each fingerprint is captured. The third step is to create the BIO+PIN by selecting the four fingers used for the BIO-PIN™ sequence then, selecting a four-digit numerical PIN for the BIO+PIN. The BIO-PIN™ application is closed and reopened to finalize the account creation/registration process. Figure 2 shows a series of screen shots of the BIO-PIN™ application the (top row from left to right) includes the Welcome page, Username and Password creation page, BIO-PIN™ fingerprint scan page, (bottom row) Sequence selection page, BIO-PIN™ successful login page and BIO+PIN™ successful login in page.

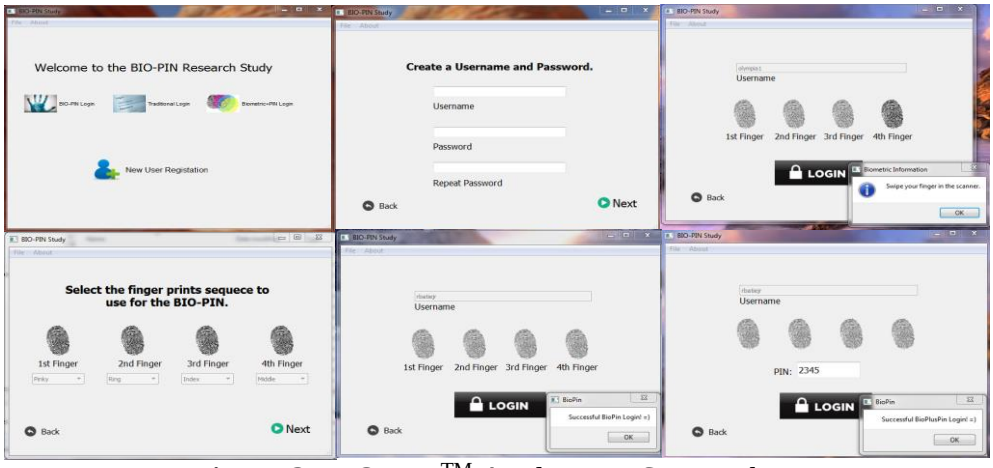

Figure 2. BIO-PIN™ Application Screen-shots

For identity verification and subsequent validation sessions, the users entered their BIO-PIN™, username/password, and BIO+PIN, into the BIO-PIN™ application. After successfully

entering the correct credentials for each method, the user is authenticated and logged in. We observed the user activities during each authentication engagement session and recorded it in the BIO-PIN™ User Information Log (data collection). The accounts creations, login attempts, fingerprints scanned successes and failures are all recorded on a hard copy of the spreadsheet and transcribed to an electronic excel spreadsheet to serve as the data for the study.

PRELIMINARY RESULTS

The preliminary results of the BIO-PIN™ study as of the submission of this paper, there were 48 users registered and actively engaged in the study going thru week nine out of the 10-weeks experiment. The study had 27 females and 21 males. The three highest numbers of members in each age group are, 36-50 (13 members), 51-55 (11 members), and 31-35 (11 members), 56+ (7 members), and 18-25 (6 members). The data showed that 86.5% of female users and 76.1% of males who participated in the study worked with computer 5-8 hours per day. Table 1 shows some preliminary details of the demographic make up of the study participants including gender, age group, user's computers experience, and number of accounts. Table 1 provides details on the number of successful login attempts by gender, age, and frequency of IT usage over time from login session 2 through login session 4. The percent and frequency of computer use column represents the percentage of users who used computers 5-8 hours per day for female and male users. Since the percent was so high, no further details were provided at this time. Additionally, the number of accounts users have that required authentication is 16+ accounts - 21 users (43.75%), consisting of 10 females and 11 males; 6-10 accounts - 17 users (35.36%), consisting of 8 females and 9 males; and 11-15 accounts (12.48%), consisting of 7 females.

Table 1. User Demographic Data Collection (N=48, as of week nine out of 10-wks)

Demo graphics	Female	Male	Total Number of Participants	Login 2 Attempt BIO-PIN (S/F)	Login 2 Attempt Pswd (S/F)	Login 2 Attempt BIO+PIN (S/F)	Login 3 Attempt BIO-PIN (S/F)	Login 3 Attempt Pswd (S/F)	Login 3 Attempt BIO+PIN (S/F)	Login 4 Attempt BIO-PIN (S/F)	Login 4 Attempt Pswd (S/F)	Login 4 Attempt BIO+PIN (S/F)
Female	**27**			**15**	**11**	**17**	**13**	**7**	**16**	**14**	**8**	**14**
Male		**21**		**15**	**12**	**20**	**12**	**9**	**17**	**9**	**4**	**12**
Total				**30**	**23**	**37**	**25**	**16**	**33**	**23**	**12**	**26**
18-30	3	3	6	6	4	6	4	3	4	2	2	3
31-35	8	3	11	9	6	9	8	5	9	8	5	6
36-50	8	5	13	7	4	10	5	2	10	3	3	7
51-55	5	6	11	4	5	5	5	2	6	6	0	5
56+	3	4	7	4	4	7	3	4	4	4	2	5
				30	**23**	**37**	**25**	**16**	**33**	**23**	**12**	**26**

Table 2 provides details of the total number of login Success/Failure. The "S" is used for *Success* and "F" for *Failure* with each authentication method. The users are allowed up to five login attempts. For each successive failed attempt an additional "F" is recorded (i.e., FFS, two failures "FF" then "S" success) until the user logs in correctly or exhausts the number of login attempts (i.e., FFFFF). A numerical value of 10 is assigned for the first successful ("S") login and each failed attempt deducts two points. This assigned login value is used for statistical calculations.

Table 2. Total Number of User Login Success and Failure (N=48, as of week 9 out of 10 Weeks)

		User Login week 2			User Login week 5			User Login week 9		
Login Values	Login Success/ Failure	BIO-PIN	Username/ password	BIO+PIN	BIO-PIN	Username/ password	BIO+PIN	BIO-PIN	Username/ password	BIO+PIN
10	S	30	23	37	25	15	33	23	12	26
8	F	13	6	6	17	13	9	13	14	15
6	FF	4	12	3	4	7	3	8	7	4
4	FFF	1	4	2	2	7	2	3	9	3
2	FFFF	0	1	0	0	5	1	1	5	0
0	FFFFF	0	2	0	0	1	0	0	1	0
	Total Users	48	48	48	48	48	48	48	48	48

CONCLUSIONS AND DISCUSSIONS

Preliminary analysis of the BIO-PIN^{TM} study data suggests that some users in all demographic distribution had difficulties remembering authenticators, primarily the username and industry standard password. The analysis from the top three members groups (age groups 31-35, 36-50, and 51-55) shows that age was not a differentiating factor when it comes to the

number of successful logins over time base on the number of participants in the groups. The gender demographic data suggests that women were more successful than men with login attempts over the sessions conducted. As of the current preliminary data, the method with the most number of successful attempts shows that the BIO+PIN was easiest to remember, followed by BIO-PIN™. It appears that users were having the most difficulty remembering their industry standard password more than any other method. Detailed analysis of the research questions and the hypothesis will be provided upon at the completion of the study.

REFERENCES

Biddle, R., Chiasson, S. and Van Oorschot, P. C. 2012. "Graphical passwords: Learning from the first twelve years." *ACM Computer Survey vol. 44, no. 4,* pp. 1-41.

Dhamija, R. and Dusseault, L. 2008. "The seven flaws of identity management usability and security challenges." *IEEE Security & Privacy*, 1540-7993/08/, pp. 24-29.

Ellis, T. J. and Levy, Y. 2009. "Towards a guide for novice researchers on research methodology: Review and proposed methods". *Issues in Informing Science and Information Technology, 6*, pp. 323-337.

Forget, A. and Biddle, R. 2008 *Memorability of Persuasive Passwords* CHI 2008, April 5 – April 10 2008, Florence, Italy.

Furnell, S. 2007. "An assessment of Website password practices." *Computers & Security, 26* (7 and 8), pp. 445-451.

Furnell, S. M., Dowland, P. S., Illingworth, H. M. and Reynolds P. L. 2000. "Authentication and supervision: A survey of user attitudes, computers and security," *Computers & Security,* 19(6) pp. 529-539

Gajek, S., Löhr, H., Sadeghi, A. R., Winandy, M. and Görtz, H. 2009. "TruWallet: Trustworthy and migratable wallet-based web authentication." *Proceedings of the 2009 ACM workshop on scalable trusted computing*, New York. pp. 19-28.

Gouda, M. G., Liu, A. X., Leung, L. M. and Alam, M. A. 2007. "SPP: An anti-phishing single password protocol." *Computer Networks*, *51*(13), 3715-3726.

Hermann, D. S. (*2002*). "*A guide to security engineering and information assurance."* Boca Raton, FL: Auerbach. Chapter 6.

Hisham A.A., Harin, S. and Sabah J. 2010. "Multi-Factor Biometrics for Authentication: A False Sense of Security." *Department of Applied Computing University of Buckingham*, MK18 1EG, United Kingdom.

Jain, A. K., Ross, A. and Pankanti, S. 2006. "Biometrics: a tool for information security." *Information forensics and security, IEEE transactions on information forensics and security 1*(2), pp.125-143.

Levy Y. and Ellis T. 2011. "A Guide for Novice Researchers on Experimental and Quasi-Experimental Studies in Information Systems Research Interdisciplinary." *Journal of Information, Knowledge, and Management Volume 6, 2011,* pp. 152-160.

Levy, Y., Ramim, M. M., Furnell, S. M. and Clarke, N. L. 2011. "Comparing intentions to use university-provided vs. vendor-provided multi-biometric authentication in online exams." *Campus-Wide Information Systems, 28*(2), pp.102-113.

Maty´aˇs, V. and ˇ R´ıha, Z. 2010. "Security of biometric authentication systems." *Computer information systems and industrial management applications (CISIM) International Conference.* Krackow, Poland, pp. 19-28.

Mirante, D. and Cappos J. 2013. "*Understanding Password Database Compromises*" Department of Computer Science and Engineering, Technical Report TR-CSE-2013-02 9/13/2013.

Ren, X. and Wu, X. 2012. A novel dynamic user authentication scheme. *International Symposium on Communications and Information Technologies,* Gold Coast, Queensland, Australia, pp. 713-717.

Ross, A. A. 2007. "An introduction to multi-biometrics." *Proceedings of the 15th European Signal Processing Conference (EUSIPCO),* vol (ed), (20-24). (Poznan, Poland)

Ross, A.A., Nandakumar, K. and Jain, A. K. 2006. "*Handbook of multi-biometrics*." New York, NY: Springer. Chapter 4.

Shenk, M. 2007. "Who can you trust, *Computer Weekly," vol* (ed), pp. 28-28. Retrieved from http://connection.ebscohost.com/c/editorials/25040622/who-can-you-trust

Solove, D. J. 2008. "The New vulnerability: Data security and personal information." Chander, A., Gelman, L. and Radin, M. J., (Eds.) *Securing privacy in the Internet age,* Stanford University Press Stanford, CA, USA pp. 111- 136.

Woodard D. and Flynn, P. 2005. "Finger surface as a biometric identifier." *Computer Vision and Image Understanding*, V100, Issue 3, December 2005, pp. 357-384.