2016

Assessing the Effectiveness of a Fingerprint Biometric and a Biometric Personal Identification Number (BIO-PIN™) when used as a Multi-Factor Authentication Mechanism

Robert B. Batie
Nova Southeastern University, rbatie@verizon.net

Assessing the Effectiveness of a Fingerprint Biometric and a Biometric Personal Identification Number (BIO-PIN™) when used as a Multi-Factor Authentication Mechanism

By

Robert B. Batie Jr.

A Dissertation in partial fulfillment of the requirements
for the degree, of Doctor of Philosophy
In
Information Systems

College of Engineering and Computing
Nova Southeastern University

2016

We hereby certify that this dissertation, submitted by Robert Batie, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Yair Levy, Ph.D. Date
Chairperson of Dissertation Committee

Peixiang Liu, Ph.D. Date
Dissertation Committee Member

Steve Furnell, Ph.D. Date
Dissertation Committee Member

Approved:

Yong X. Tao, Ph.D., P.E., FASME Date
Dean, College of Engineering and Computing

College of Engineering and Computing
Nova Southeastern University

2016

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Assessing the Effectiveness of a Fingerprint Biometric and a Biometric Personal Identification Number (BIO-PIN™) when used as a Multi-Factor Authentication Mechanism

By
Robert B. Batie Jr.
December 2016

The issue of traditional user authentication methods, such as username/passwords, when accessing information systems, the Internet, and Web-based applications still pose significant vulnerabilities. The problem of user authentication including physical and logical access appears to have limited, if any, coverage in research from the perspective of biometric as ‘something the user knows.’ Previous methods of establishing ones’ identity by using a password, or presenting a token or identification (ID) card are vulnerable to circumvention by misplacement or unauthorized sharing. The need for reliable user authentication techniques has increased in the wake of heightened concerns about information security and rapid advancements in networking, communication, and mobility.

The main goal of this research study was to examine the role of the authentication method (BIO-PIN™ or username/password) and time, on the effectiveness of authentication, as well as the users’ ability to remember the BIO-PIN™ versus username/password (UN/PW). Moreover, this study compared the BIO-PIN™ with a traditional multi-factor biometric authentication using multiple fingerprints (without sequence) and a numerical PIN sequence (noted as "BIO+PIN"). Additionally, this research study examined the authentication methods when controlled for age, gender, user’s computer experience, and number of accounts. This study used a quasi-experimental multiple baseline design method to evaluate the effectiveness of the BIO-PIN™ authentication method. The independent, dependent, and control variables were addressed using descriptive statistics and Multivariate Analysis of Variance (MANOVA) statistical analysis to compare the BIO-PIN™, the BIO+PIN, and UN/PW authentication methods for research questions (RQs) 1 and 2. Additionally, the Multivariate Analysis of Covariance (MANCOVA) was used to address RQ 3 and RQ4, which seeks to test any differences when controlled by age, gender, user experience, and number of accounts. This research study was conducted over a 10-week period with participant engagement occurring over time including a registration week and in intervals of 2 weeks, 3 weeks, and 5 weeks. This study advances the current research in multi-factor biometric authentication and increases the body of knowledge regarding users’ ability to remember industry standard UN/PWs, the BIO-PIN™ sequence, and traditional BIO+PIN.

Acknowledgments

First I would like to thank God for blessing me with the mental capacity, physical health, endurance and tenacity to undertake this once in a lifetime challenge. The Lord knows my struggles, my pain, my evil and my heavenly ways and still he blessed me with all I have ever asked for even if it were not good for me. Oh, the lessons I've learned and the debt I owe.

I'd like to thank my loving wife who is my biggest cheerleader and greatest fan. Thank you for your love, patience, and support.

I acknowledge and thank my Dissertation Chair, Dr. Yair Levy, who orchestrated my success with his wisdom, guidance, humor, temperament, and patience. From the first moment I sat in your class you opened my eyes to what it means to succeed in this endeavor. You are brilliant, funny, tough, patient and tenacious. You pushed me to work harder and reach farther in my journey for this terminal and most powerful degree, the Ph.D. I'd also like to think my Dissertation Committee, Dr. Stephen Furnell, who always challenged my ideas and made me see things from a different perspective, and Dr. Peixiang Liu whose attention to detail caused me to double check my actions and intent. I'd like to thank Alen Cruz and Sylvia Traxler, my Twin Pro Software Development team who believed in the BIO-PIN™ concept and gave me an unbelievable application to address my research questions and test my hypothesis. It is always my pleasure and privilege to work with you two in any circumstance. You made it look so easy and fun. Your attitudes are infectious!

Additionally, to all those who participated in the BIO-PIN™ Study, your unselfish commitment to the project and its inconveniences are worth their weight. I was so honored that you would take time to help me fulfill my life-long dream and take part in this once-in-a-life-time cutting edge project. To each and everyone, thank you! Finally, I thank the legacy Bobby, Janice, Taja, Demontinah, BJ, and Brockton, from whom I draw inspiration in hopes that I may inspire them to step out of the boat beyond their comfort zone and walk by faith to seek knowledge of the world and higher learning. Lead by example. I love you all!

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Much attention has been given to the problem of user authentication for the Internet and Web-based applications, including physical and logical access (Woodard & Flynn, 2005). Previous methods of establishing one's identity by using a password, or presenting a token or identification (ID) card are vulnerable to circumvention by misplacement or unauthorized sharing. According to Maty´aˇs and ˇ R´ıha (2010), one of the primary advantages of biometric authentication methods is that fingerprints and other biometric modalities are unique and permanent human physiological characteristics. Users cannot share their biometric characteristics as easily as they do their passwords or tokens (Furnell, Dowland, Illingworth, & Reynolds, 2000). Biometric characteristics are not easily compromised in the same way a user's password might be (Maty´aˇs &ˇ R´ıha 2010).

Biometric modalities such as fingerprints and handprints have long been used as biometric identifiers in other research efforts. Ross (2007) as well as Jain, Ross, and Pantkanti, (2006) have done extensive work establishing identity using biometric feature mosaicking, feature-level fusion, multi-biometric systems, as well as two-dimensional (2-D) measurements of the fingers and hand. Woodard and Flynn (2005) used a similar approach with finger surface features for personal identification. This study built on these previous scholarly works as well as research conducted by Hayashi, Christin, Dhamija, and Perrig (2008), where users authenticate by selecting a series of pictures in a sequence—'something the user knows.'

This dissertation is organized in the following manner. It begins with the problem statement followed by specific research goals, the research questions, and hypothesis. It continues with sections on the relevance and significance of this study, as well as a literature review. Next, it discusses barriers, issues, assumptions, and limitations. Finally, it discusses the research approach, and the resources required to conduct this study.

Problem Statement

The research problem this study addressed was that traditional user authentication methods, such as username/password (UN/PW), pose a significant vulnerability when accessing information systems (Furnell, 2007). User knowledge of creating adequate passwords (training), the complexity and makeup of the password, and the process for resetting the passwords varied across organizations. Usernames and passwords are very cheap to implement as all operating systems come with the capability to use them for authentication. Further, Furnell (2011) suggested that users were having trouble remembering passwords and were probably frustrated with the password process. The management of these authentication methods is still evolving (Furnell, 2011).

Since Furnell's study in 2007, he conducted a follow-on study in 2011. The follow-on study concluded that little improvement in password practices had occurred even with the increased use of online services and computer breaches. The problems of password vulnerability and compromise became more acute as Internet use grew and fraudulent strategies were launched in an effort to exploit the lack of adequate Internet authentication (Shenk, 2007). Ren and Wu (2012) defined authentication as "the act of confirming that the communicating entity is the one claimed" (p.714). Hermann (2002) defined authentication as "a way to establish, verify, and prove the validity of a claimed identity of a user, process, or system" (p. 43). Authentication is usually accomplished by one or more of the following methods: (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 physical attributes or traits (i.e., fingerprint, face, voice recognition, or iris biometric) (Hisham, Harin, & Sabah, 2010).

Each of these traditional methods of authentication has shortcomings that suggest these methods are inadequate. According to Zhang (2004) weaknesses exist in something the user knows and something the user has because they are not based on any inherent attribute of the user in the process. Biometric offers a natural and reliable solution to certain aspects of authentication using inherent physical attributes (Ross, 2007). According to Ross (2010), biometrics is the science of establishing identity by using physiological features, characteristics, or traits (such as fingerprints, retina venial patterns, irises, voice, face patterns, as well as hand/finger measurements) for identification and authentication purposes. According to Ross, Nandakumar, and Jain (2006), Web-based services such as e-banking, e-commerce, e-government, electronic medical records, online learning, and the decentralized services for processing credit card transactions have further enhanced the need for reliable identity/authentication management systems.

In 2013, Apple added the option of a fingerprint application for authentication to its new version of the iPhone 5s allowing users to move away from traditional PIN authentication (Lemos, 2013). The problem with this implementation is that the Chaos Computer Club (CCC) and others have hacked the single fingerprint biometric on the iPhone 5s to show that a persistent bad actor can take over the iPhone in a series of steps. First, the persistent bad actor must obtain the iPhone and disconnect it from the Internet using airplane mode in case the original owner implements the “find-my-iPhone” feature. Next, the bad actor creates a high-resolution photocopy (2400dpi) and wood glue spoof of the owner’s fingerprint to unlock the iPhone. The bad actor then hijacks the email accounts where password reset information will be sent. The persistent bad actor must disconnect and reconnect the iPhone from the Internet long enough to receive information necessary to reset the iPhone but not long enough for the “find-my-iPhone” feature to successfully locate the device (Chaos Computer Club, 2014). Although this is a more complicated process than simply shoulder-surfing to acquire a user’s PIN, it is possible and has been accomplished by the Chaos Computer Club.

Whether the fruit of attempting to compromise the iPhone 5s’s iTouchID is worth the effort depends on the motive of the hacker(s). CCC’s motive appears to have been just to prove that the iTouchID could be breached as opposed to gaining any significant information. This type of attack may be impractical except for high-value, high-yield targets like acquiring the little black book of a spy, or a gateway to other accounts. Besides the potential value of the information, how perishable is the potential yield? Surely the owner of the phone will report the device as lost or stolen and commence procedures to protect the information and recover the phone. Moreover, there are nine steps that must be executed in correct order to compromise the device. If the hacker misses any step, the hacker may not be successful. Built-in features begin with the failure to present acceptable credentials. After five attempts, the phone will ask for a passcode. For extra security, the iPhone 5s also has a setting that will completely wipe the device clean after 10 failed fingerprint unlock/passcode unlock attempts (Wehner, 2013). Apple allows users to register up to five separate fingerprints that can be used to unlock the device. Once a print is registered, Touch ID allows the person three tries with the fingerprint sensor before it prompts the user to input a 4 to 6-digit PIN instead. While the feasibility of spoofing the iPhone 5s iTouchID using the photocopy and wood glue is possible, it is unlikely (Wehner, 2013).

Maty´aˇs and ˇR´ıha (2000) classified biometric systems into four levels: level one comprises very simple systems; level two, simple systems; level three, intermediate systems, and level four, advanced systems. The iPhone 5s iTouchID is a level two biometric device because no aliveness test or tamper resistance feature is required, and a traditional authentication method is offered in the case of biometric system malfunction or suspected compromise. Biometric authentication devices up to level two devices are among the easiest to successfully attack because they have no way of validating the person is alive (Maty´aˇs & ˇR´ıha 2000).

Ross et al. (2006) observed that differentiating between an authorized person and an impostor who has acquired the token or knowledge of the person's password is difficult for most information systems. The implication is that tokens and passwords can be lost, stolen, or forged. Hong, Jain, and Pankanti (1998) stated that, unlike possession and knowledge-based identity authentication schemes, biometric identifiers could not be easily misplaced, forgotten, or guessed. A strong authentication strategy is essential for implementing effective access control rights and privileges (Ross et al., 2006).

Singh (2008) observed that information security is becoming more important to data owners and users since today's computers store increasingly sensitive and valuable information. If these information systems are compromised, it could harm national security, damage reputations of corporations and individuals, or violate privacy laws (Solove, 2008). Strong user authentication techniques must be employed to prevent unauthorized access to information systems (Cavoukian, 2005). Singh (2008) observed that although user authentication is only one element in the overall security of information systems and data protection, it is among the most important. Without access to sensitive data, intruders may cause only minimal damage to information systems (Singh, 2008). Moreover, identity theft has become one of the fastest growing crimes on the Internet leading to huge financial losses and privacy concerns because of rising online fraud and software attacks (Gajek, Löhr, Sadeghi, Winandy, & Görtz, 2009). In most cases, the perpetrator is often a knowledgeable insider (Ross et al., 2006; Tipton & Krause, 2012).

According to Hisham, Harin, and Sabah (2010), randomly generated, or one-time passwords, can offer a reasonably sufficient security mechanism for user authentication. In practice, secret passwords that humans can remember are usually short and easy to guess (Hisham et al., 2010). For example, a survey of 1,200 British office workers conducted by CentralNic in 2001 found that nearly 50% of the workers chose their own name, a pet's name, or a family member's name as a password (Hisham et al., 2010). Others chose their passwords based on celebrity or movie character names. Such passwords can be guessed by running a simple brute force or dictionary attack (Hisham et al., 2010). Recently, some operating systems, applications, and web browsers (i.e., Microsoft Windows®**,** MSN, and Google®) began providing a password strength indicator capability to help users create stronger passwords (Furnell, 2007; Furnell 2013). However, such increased demand on the complexity of passwords can have a negative impact on users completing tasks, or users may have trouble remembering a more complex password and change it back to a simple password (Mujeye & Levy, 2013).

Rajput, Chen, and Hsu (2005) observed that access to information systems needing protection from unauthorized users is controlled by having users prove their identity with various authentication mechanisms. For many years, banks used 4-digit PINs and cards (two-factor model) for customer authentication at automated teller machines (ATMs). Most gas stations have implemented two-factor transactions with credit card use by requiring the customer to input the zip code (or PIN if it is a debit card), associated with the user's billing address to complete the transaction. With so many different approaches to authentication, coupled with the number of breaches, compromises, and incidents of identity theft, authentication is still a major problem (Ross et al., 2006). Woodard and Flynn (2005), Furnell (2013), and Mujeye and Levy (2013) observed that personal identification continues to be a problem of interest to many researchers. Thus, additional research on new and more effective authentication methods, including two-factor and multi-factor authentication methods, appear to be warranted.

Research Goals

This research study addressed a main goal and several specific research goals. The main goal was the role of the authentication method (BIO-PIN™, BIO+PIN, & UN/PW) and time (i.e. the amount of time that has passed since the BIO-PIN™, BIO+PIN, & UN/PW was created for each user) on the effectiveness of authentication, as well as the users' ability to remember the BIO-PIN™ versus the BIO+PIN versus UN/PW.

Industry standard complex passwords consist of a combination of eight or more characters that include uppercase letters, lowercase letters, numbers, and special characters (Dhamija & Dusseault, 2008). Password creation and password security are only part of the problem with password usability. User training and memorability are also part of the equation when it comes to password construction and security. Users have to remember multiple passwords for access to different applications and they are required to change passwords frequently due to password expiration mechanisms. These factors attribute to the users' inability to remember complex passwords causing the user to write it down, seek variations of the same password, or create simple passwords that are easy to guess or crack. These exercises increase insecure work practices according to Forget and Biddle (2008). These methods actually decrease password memorability due to within-list interference causing users to write down passwords, which of course, compromises password security levels. Dictionary words and names are the most vulnerable forms of passwords.

The simplest and cheapest authentication technique widely used for the purpose of authentication is password-based schemes. Though simple in implementation, password-based schemes are vulnerable to password guessing attacks, replay attacks, dictionary attacks, and social engineering attacks. To reduce the chances of guessing attacks, a user can choose a long and complex password that is difficult for the user to remember (NIST SP 800-118, April 2008). Replay attacks can be curbed to an extent by using encrypted passwords. One-time passwords, where the passwords for each login are unique and randomly generated numbers, are a better authentication technique. These one-time passwords can be combined with smart cards to build a secure solution. But this is not the optimal solution as it can be invaded by man-in-the-middle and man-in-the-browser attacks, and is time consuming. Moreover, passwords or PINs are likely to be forgotten, copied, or stolen, and subsequently used malevolently by an imposter. Smart cards are more secure than the other aforementioned techniques due to their public key infrastructure (PKI); however, they are also susceptible to loss or theft and can be used for unauthorized access. The third possibility, biometrics, can provide stronger authentication and non-repudiation, as it is unique to an individual. Biometrics is hard to copy, replicate, or deny, and cannot be easily stolen. Biometrics can be integrated with the smart card to build a more stable, and secure user authentication system.

Menezes, Van Oorschot, and Vanstone (1996) described password security in terms of password spaces: the total number of distinct passwords that can be created with a given set of characters. The 95 English U.S. keyboard characters are usually split into four types of password spaces: lowercase letters (26), uppercase letters (26), digits (10), and symbols (33). Password security can be measured by the number/length of characters and the number of password spaces. For example, the password “robert ” is six characters long and contains only lowercase letters; therefore, it offers 266 ≈ 3.1 Å~108 ≈ 28.2 bits of security. Similarly, “robert123” has 9 characters and contains lowercase letters and digits; therefore, it offers 369 ≈ 1.0Å~1014 ≈ 46.5 bits of security. Capitalizing an “r” (“Robert123”) boosts the security to 629 ≈ 1.3Å~1016 ≈ 53.6 bits.

Forget and Biddle (2008) noted that passwords constructed this way are still insecure because they are composed of dictionary words and a predictable number sequence that can be easily guessed by most password attack tools. Security professionals often attribute weak passwords to a lack of user effort, knowledge, and motivation. Forget and Biddle

(2008) also argued that users misunderstood the security threats and how to effectively defend themselves with the given mechanisms. Moreover, human memory limitations further prevent users from utilizing the full theoretical security potential of passwords (Forget & Biddle, 2008).

Table 1, *Summary of Organizational User Database Compromises,* provides some examples of user database compromises described by Mirante and Cappos (2013). It lists the organization and the type of system where usernames and passwords were compromised, the date of the reported incident, as well as a URL where additional information may be found. It also lists cases with the approximate number of users affected by the compromise. While Mirante and Cappos (2013) lists over 34 breaches, including Sony Pictures, Linkedin, Twitter, the New York Times, Evenote, and Apple, only six are discussed in Table 1.

As a result of the compromises examined in the Mirante and Cappos (2013) study mentioned in Table 1, many sites are migrating to two-step/two-factor authentication or offering it as an option. A list of some vendors who are offering two-factor options are Evernote, Dropbox, Twitter, Google, Facebook, Yahoo Mail, and PayPal. Additionally, most major banking institutions either require its use or offer it as an option. Two-step authentication may require the user to enter a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA$^{\text{TM}}$), a type of challenge-response test used in computing to determine whether or not the user is human, or receive a message via cell phone and enter a PIN or other piece of information only the user knows at the time of the transaction. It may also involve entering the answers to questions the user selected and answered during either account creation or site enforced maintenance (Mirante & Cappos 2013).

Table 1. Summary of Organizational Database Compromises (Mirante & Camppos 2013)

Organization	Compromise
Barracuda Networks (July 24, 2013)	A vulnerability in Barracuda update servers was found that allowed access to all employee login credentials. An Egyptian security advisor Ephrahim Hegazy discovered the flaw. The servers were misconfigured and stored password information within the web directory, rather than outside of it. All username/password information was stored in plaintext. The vulnerability was fixed before any exploits could occur. http://thehackernews.com/2013/07/Barracuda-network-Password-disclosure-vulnerability_24.html
Simple Machines Forum (July 20, 2013)	Credentials stolen from another website were used to log in to an administrator account. Admin privileges permitted the hacker to dump the site's user database, which included passwords, personal messages, and other information. All users were advised to change their passwords. http://www.simplemachines.org/community/index.php?topic=508232.0
Ubisoft (June 28, 2013)	Hack exposed user names, encrypted passwords, and email addresses for potentially 58 million users. Hack was initiated using stolen credentials. https://support.ubi.com/en-GB/FAQ.aspx?platformid=60&brandid=2030&productid=3888&faqid=kA030000000eYYxCAM
Ubuntu Forums (July 14 and July 20, 2013)	Email addresses, usernames, and passwords for 1.82 million accounts were exposed. The passwords were hashed using MD5 and a per-user cryptographic salt was used. This scheme is considered by experts to be an inadequate means of password protection. http://arstechnica.com/security/2013/07/hack-exposes-e-mail-addresses-password-data-for-2-million-ubuntu-forum-users/
Nintendo (June 9 to July 4, 2013)	The Japanese Club Nintendo site was attacked via brute force by unknown attackers. Login credentials stolen from other sites were used to gain access. Over 15,000,000 attempts were made with 23,926 being successful. Nintendo realized the attack was in progress after observing a huge number of login errors and reset the affected user's passwords: http://hothardware.com/News/Hacked-24000-Club-Nintendo-Accounts-Compromised/ and http://nakedsecurity.sophos.com/2013/07/09/nintendo-cracks-after-month-long-15-5-million-strong-hacker-bombardment/ The accounts experiencing illegal access had the user's names, addresses, phone numbers, and email addresses compromised. http://threatpost.com/brute-force-attack-on-nintendo-fan-site-yields-data-on-25k No information concerning where the login information used in the attack originated from could be found.
LivingSocial (April 26, 2013)	50,000,000 customers were impacted by the exposure of customer names, email addresses, birth dates, and encrypted passwords. http://allthingsd.com/20130426/livingsocial-hacked-more-than-50-million-customer-names-emails-birthdates-and-encrypted-passwords-accessed/

Because of the breaches and compromises of a large number of computer systems' databases, which included usernames/password and other personally identifiable information, an approach such as the BIO-PIN^{TM} might make a viable alternative to user authentication. This study compared the user's fingerprints presented to the information system in a specific sequence for authentication as the PIN. Additionally, the BIO+PIN used four fingerprints presented by the user, in any order, and a numerical PIN entered in a specific sequence. The aim of this study was to test which authentication method would be easier to remember and thus, provide a more effective method of authentication to information systems.

The effectiveness of a biometric mechanism is a performance parameter determined by the False Match Rate (FMR) and False Non-Match Rate (FNMR), which directly measure biometric recognition (Biometric Evaluation Methodology, 2002). It is similar to system performance that is expressed in the parameters of False Accept Rate (FAR) and False Reject Rate (FRR). The aim of this study was to assess the effectiveness of the BIO-PIN™ authentication method. BIO-PIN^{TM} uses unique identifying features entered in a specific sequence. This study sought to determine if users could more easily remember the BIO-PIN™ sequence versus an industry standard complex password or the BIO+PIN sequence. Fingerprints entered out of sequence or not recognized by the authentication mechanism could cause a FAR/FRR. This may be compensated for by the knowledge that the sequence the fingerprints were presented, were within the established threshold.

Jain et al. (2006) argued that the need for reliable user authentication techniques have increased in the wake of heightened concerns about security and rapid advancements in networking, communication, and mobility. Dhamija and Dusseault (2008) also stated that many users today are faced with the burden of managing an increasing number of authenticators, which in some cases has led to password fatigue (p. 25). According to Dhamija and Dusseault (2008), password fatigue (p. 25) is a condition where users are over burdened with managing an increasing number of passwords to access different types of information. On average, users have approximately 25 accounts that require passwords, and they can type eight passwords per day to access the various types and sensitivities of data (Dhamija & Dusseault, 2008). According to Gouda, Lie, Leung, and Alam (2007), many people have multiple accounts on the Internet such as Webmail, travel accounts, online stock trading, online banking, and online shopping. They estimated that users can access as many as 15 accounts with username and password on a daily basis. They were faced with the dilemma of creating simple, easy to guess passwords since they had so many to remember or writing down the more complex passwords because they were too difficult to remember. Users will take the path of least resistance which can lead to compromise by creating passwords that are so simple that they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks (Jain, et al., 2006). Since users typically can only remember four to five different complex passwords effectively, some users feel overwhelmed by the increasing number of usernames and unique complex passwords they are required to use and remember (Dhamija & Dusseault, 2008; Gouda et al., 2007). According to Jain et al. (2006), Furnell, (2013), and Splash data 2015, one of the most commonly used password is still the word "password."

To strengthen the username and password concept, two-factor or multi-factor authentication methods may be used. Using the two-factor authentication method, users present at least two different pieces of evidence to identify and validate that they are who they claim to be (Hanche, Berti, & Hare, 2004). Most often, multi-factor authentication is a combination of something the user is, knows, and/or has. Multi-factor biometrics such as the BIO-PIN™ uses fingerprints in two ways: something the user has and something the user knows (the sequence entered). Figure 1 illustrates the BIO-PIN™, authentication system, which consists of fingerprint and finger PIN sequencing concept of BIO-PIN™, a fingerprint reader and a standalone laptop computer that contains the BIO-PIN™, authentication application. The fingers were numbered from one to five, starting with the thumb (F1 or T). During the study, most of the participants referred to their fingerprints by the first letter of the name of the finger. The fingers are referred to as: index finger (F2, or I), the middle finger (F3 or M), the ring finger (F4 or R), and the pinky finger (F5 or P). This finger identification could apply to either the left or right hand. In this case, for example, the left thumb could be identified as F6, and right index finger could be F7, and so on.

Each finger is made up of three phalanges (proximal, middle, & distal) or finger-segments, and fingertips. The fingertips (fingerprints) were placed on the reader in specific order to represent the individual's selected sequence (i.e. PIN). This sequence could be illustrated as PRMI, TIMR, or any combination.

The fingertips were used as a key element in this study to illustrate the BIO-PIN™ authentication methods. The proximal and middle phalanges, for the purpose of this study, were defined as finger-segments between the fingertips and the palm. While existing technology makes the measurement of these segments possible, the cost is high and, thus, beyond the scope of this study. This research investigated the strength of the fingertip fingerprint when used as part of the BIO-PIN™.

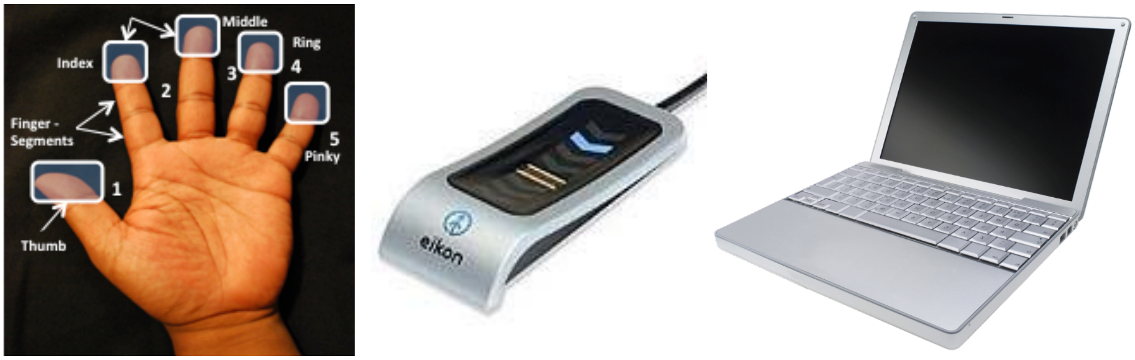


Figure 1. BIO-PIN Authentication System (BIO-PIN Sequence, Fingerprint Reader and Laptop Computer

After attending the International Biometric Conference vendor presentation on various Biometric fingerprint products, several fingerprint scanner devices such as Digital Persona 4500 series U.are.U models were considered. The Eikon series fingerprint scanners were selected based on cost, convenience, portability, operating system compatibility, and the inclusion of the Software Development Kit (SDK). Three fingerprint readers were provided as part of this study: two single print reader(s) (Eikon 710; Eikon 510) and one single swipe fingerprint reader (Eikon II).

The most commonly used fingerprint readers today are optical scanners or capacitance scanners. Each work on the principals of a charge-coupled device (CCD)—the same light sensor system used in digital cameras and camcorders. The optical scanner uses a CCD and is simply an array of light-sensitive diodes called photosites, which generate an electrical signal in response to light. Each photosite records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (i.e. a finger).

The Authentec™ Biometric Evaluator software application was used to evaluate the capabilities of the fingerprint module. This application supports the biometric modules and chipsets including the Embedded Strip System (ESS), Trusted Fingerprint Module (TFM), and Sensor Only Solution (SONLY). This tool has an intuitive graphical user interface (GUI) that makes it easy for users to navigate through the application, calibrate the Eikon fingerprint readers, and validate and verify the fingerprint reader connection and the registered user's fingerprint. The Eikon fingerprint reader connection was calibrated and verified before each login session. Checking the calibration of the fingerprint reader prior to each login session minimized false readings and errors when presenting fingerprints to the application.

Goals

The first specific goal this research study addressed was to assess the role of authentication using a fingerprint biometric template to validate the user and achieve a low FAR when the correct sequence of the BIO-PIN™ fingerprints was entered for authentication. The second specific goal this research study addressed was to assess the role of authentication using a fingerprint template to validate the user and achieve a low FRR when the correct sequence of the BIO-PIN™ fingerprints was entered for authentication. The first and second goals led directly to how effective fingerprints are (as measured by the FAR and FRR and finding the Relative Operational Characteristic [ROC]) as a multi-factor biometric when used to authenticate information systems' users.

The third specific research goal this research study addressed was to test if there were any differences in the ability of users, based on age, gender, number of computer accounts, or computer user experience, to remember their BIO-PIN™. The matrix in Table 3 compares the UN/PW, the BIO-PIN™, and the BIO+PIN methods over a 10-week period during weeks zero, two, five, and ten. Table 3 illustrates the authentication comparison matrix and the evaluation method for this goal.

The BIO-PIN™ sequence and the BIO+PIN illustrated in Table 3 are different in that the BIO-PIN™ sequence requires the users to present their fingerprints to the authentication mechanism in a specific sequence that only the user knew (such as IMRP or TRIM). The BIO+PIN required the user to enter their fingerprint biometric in any order plus an additional four-digit numerical PIN (i.e. 1234) in a sequence. The BIO-PIN™ sequence versus the BIO+PIN versus UN/PW was measured over time by analyzing the number of times the user successfully authenticated over time, based on spreadsheet entries by the principal investigator as well as audit records.

Table 2. Authenticator Comparison Matrix.

	Time			
	Week 0	**Week 2**	**Week 5**	**Week 10**
Hypothesis				
H3a /H4a-d	UN/PW	UN/PW	UN/PW	UN/PW
H3b /H4a-d	BIO-PIN	BIO-PIN	BIO-PIN	BIO-PIN
H3c/H4a-d	BIO+PIN	BIO+PIN	BIO+PIN	BIO+PIN
H3d /H4a-d	UN/PW	UN/PW	UN/PW	UN/PW
	BIO-PIN	BIO-PIN	BIO-PIN	BIO-PIN
	BIO+PIN	BIO+PIN	BIO+PIN	BIO+PIN

UN/PW =	Username/Password
BIO-PIN =	Biometric fingerprint sequence
BIO+Plus PIN =	Biometric plus 4-digit numerical PIN

Research Questions

The Research Questions this study addressed were:

RQ1: What is the role of time on the effectiveness of authentication as measured by FRR on the BIO-PIN™ authentication method?

RQ2: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, and UN/PW) on the users' ability to remember the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW?

RQ3: What is the role of *time* on the user's *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW?

RQ4: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & UN/PW) and *time* on the users' *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW when controlled for *age, gender, volume of user accounts, or frequency of IT usage*?

RQ4a: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & UN/PW) and *time* on the users' *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW when controlled for *age*?

RQ4b: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & UN/PW) and *time* on the users' *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW when controlled for *gender*?

RQ4c: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & UN/PW) and *time* on the users' *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW when controlled for *volume of user accounts*?

RQ4d: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & UN/PW) and *time* on the users' *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus UN/PW when controlled for *frequency of IT usage*?

Hypotheses

The specific hypotheses that relates to RQ3 and RQ4 noted in the null format are listed below:

H3a: There will be no significant difference in remembering an industry standard complex UN/PW over time at intervals of two (2) weeks, three (3) weeks, four (4) weeks, and over a ten (10)-weeks period.

H3b: There will be no significant difference in remembering the sequence of the BIO-PIN™ over time, in intervals of two (2) weeks, three (3) weeks, five (5) weeks, and over a ten (10)-weeks period.

H3c: There will be no significant difference in remembering the BIO+PIN over time, in intervals of two (2) weeks, three (3) weeks, five (5) weeks, and over a ten (10)-weeks period.

H3d: There will be no significant difference in remembering the BIO-PIN™ sequence versus BIO+PIN versus UN/PW over time, in intervals of two (2) weeks, three (3) weeks, five (5) weeks, and over a ten (10)-weeks period.

H4a: There will be no significant difference in remembering an industry standard complex UN/PW, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for age.

H4b: There will be no significant difference in remembering an industry standard complex UN/PW, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for gender.

H4c: There will be no significant difference in remembering an industry standard complex UN/PW, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for volume of user accounts.

H4d: There will be no significant difference in remembering an industry standard complex UN/PW, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for frequency of IT usage.

Password Authentication Method

By using the BIO-PIN™ as something the user knows and something the user has, this study assessed whether the techniques would increase the security of personal authentication, and if it could mitigate the problems of forcing users to remember many industry standard complex passwords or fingerprint biometric plus PIN.

According to Tullis and Tedesco (2005), password memory and security in user authentication has long been a concern in the computing industry. When choosing passwords, users tend to choose very easy, memorable passwords that can often be guessed. When given meaningless strings of passwords by the system, users are often unable to recall them, resulting in help-desk calls and the costs of resetting passwords (Tullis & Tedesco, 2005). With all of the passwords users use to access systems on a daily basis, users even forget the easy passwords that they have chosen for themselves—unless they use the same password for every system or write their passwords down, both of which are a security risk (Tullis & Tedesco, 2005).

Although passwords provide a minimal security inconvenience, they still offer adequate and inexpensive security for both networked and non-networked computers (Tognazzini, 2005). However, there are numerous limitations to using passwords for authentication. The most obvious problem is users often forget their passwords causing frustration and delays. Today's typical Internet user has multiple passwords to memorize and recall on demand. This memory burden leads to types of behavior that can compromise security, e.g., writing passwords down or frequently reusing them to alleviate memory limitations (Gaw & Felten, 2006; Halderman et al., 2005). Forgotten passwords also result in lost customers, lost revenue, increased administration costs, and helpdesk calls for businesses (Brown et al., 2004).

Modern digital token generators create these dynamic passcodes (One-Time-Passcode or OTP) automatically. Although these devices alleviate the memory problems of multiple passwords and are small (therefore easy to carry), they do not always extend to multiple uses. It is easy to see a situation where different tokens of this type would be required for various websites and other services. Everyday use of tokens in authentication would require possession of the device when needed, and the ability to use it. Token solutions also involve cost in rollout and support (Claessens et al. 2002).

Review of several dissertations and empirical studies revealed that a variety of demographics including age, gender, and level of experience in biometric and authentication studies have been used as part of their research. Woodard and Flynn (2005) used age and gender (male/female) and GPA. Weir et al. (2010) used a demographics questionnaire that involved age, gender, use of eBanking, locations of use, and mobile phone ownership as part of the study. The Zhang et al. (2010) empirical study on improving password recall suggested that the more passwords users have to remember the more susceptible they are to compromise by writing them down, forgetting them, or using the same password on multiple systems. All of these categories are part of the general computer user population. Further, a user's level of IT experience may affect their ability to perform certain user tasks. The more familiar a person is with tasks such as logging into a computer system, the more proficient they are at navigating through the tasks. Age and gender also affect a user's cognitive ability to remember username, password, BIO+PIN, or BIO-PIN sequences. Ultimately the general computer user population may benefit from the results of this study.

Relevance

This study is relevant because it seeks to provide insight into an area with a limited number of research studies. There don't appear to be many studies in the area of a biometric as 'something the user knows, something the user is or knows how to be'—users presenting biometric feature in a *sequence* in much the same way one would enter a PIN. This study presents a novel idea (A US Patent Pending was issued for this idea: Application No. 61/692,981): the user presents the fingerprints to the authentication mechanism in a specific sequence known only to the user and the research team. By presenting the biometric feature in this way, the method may help strengthen the authentication process, and create a higher degree of trust between the subject (user) and the object (authentication process, data, or Website).

Significance

This study is significant because it advances the current research in multi-factor biometric authentication and increases the body of knowledge regarding the users' ability to remember industry standard passwords, Biometric authentication methods (the BIO-PIN™ sequence), and traditional BIO+PIN. It continues to build on previous research conducted by:

- Hayashi, Christin, Dhamija, and Perrig (2008), who discussed secure authentication in picture recall
- Woodard and Flynn (2005), who researched finger surface as a multi-modal biometric

With the BIO-PIN™ as something the user is (a fingerprint) and something the user knows (the correct sequence the fingertip and/or finger segment are presented or selected), the user validation may be strengthened. Several researchers of note (including Furnell, 2007; Furnell, 2013; Furnell et al. 2000; Jain et al. 2006; Mujeye & Levy 2013; Woodard & Flynn 2005) and others have conducted research in this area.

Barriers and Issues

Barriers to this study included obtaining an adequate size of volunteer participants by demographics, securing Institutional Review Board (IRB) approval, and the development of the BIO-PIN™ multi-fingerprint software application. The study could be affected if participants were not properly trained on password creation and use, naturally resisted, or feared the use of their biometrics. IRB approval was obtained prior to contact with any potential participants. Participants were briefed on how their information would be used during and after the study according to the IRB policy, given training on how to create strong passwords according to the suggestions of Furnell (2007), and trained on how to use the BIO-PIN™ and the BIO+PIN authentication systems.

Assumptions, Limitations, and Delimitations

Assumptions

This study assumed the information collected from the participants such as age, gender, number of accounts, and frequency of IT usage was true and accurate. The hardware and software used in this study met Federal Communications Commission (FCC), Underwriters Laboratory (UL), and National Institute of Standards and Technology (NIST) standards of functionality, manufacturing, safety, and security. It was assumed that the hardware and software used in this study would perform as intended.

Limitations

Limitations are factors that are beyond the control and may potentially impact the internal validity of the study. The possible threat to internal validity was users generating familiar passwords. To minimize this threat, the users were trained in password creation and asked to create a totally new password based on a password creation technique (using a password scheme based on a phrase the user found easy to remember).

Delimitations

Delimitations are factors that were intentionally imposed to constrain the scope of the study to make it manageable. For this study, a small quota sample size was used to manage the study more effectively. The number of participants could impact the generalizability of the results of the study.

Definition of Terms

Attempt: The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify (Newbold, 2008).

Authentication: Alternative term for *Verification*. Authentication is a method to establish, verify, and prove the validity of the claimed identity of a user, process, or system (Hermann, 2002).

Biometrics: The science of establishing identity by using physical features, characteristics, and traits such as fingerprints, retina venial patterns, irises, voice, face patterns, and hand/finger measurements for identification and authentication purposes (Ross, 2010).

Biometric Data/Feature: The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data) (Newbold, 2008).

BIO-PIN™: The multi-factor authentication method using the fingerprint biometric as something the user is and, when entered in a particular sequence, something the user knows (Biometric Personal Identification Number (BIO-PIN™)).

BIO+PIN: The multi-factor authentication method using the fingerprint biometric and a numerical personal identification number (PIN) as something the user knows (BIO+PIN).

Biometric Sample: Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint) (Newbold, 2008).

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA™): An acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". A type of challenge-response test used in computing to determine whether or not the user is human.

Comparison: The process of comparing a biometric sample with a previously stored reference template or templates (AfB, ICSA).

Enrollee: A person who has a biometric reference template on file in the biometric authentication database (AfB, ICSA).

Enrollment: The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity (AfB, ICSA).

Equal Error Rate (EER): The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances (AfB, ICSA).

Extraction: The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template (AfB, ICSA).

False Acceptance: When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity (AfB, ICSA).

False Acceptance Rate (FAR): The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The FAR may be estimated by FAR = NFA/NIIA or FAR = NFA/NIVA where:

- NFA is the number of false acceptances.
- NIIA is the number of impostor identification attempts.
- NIVA is the number of impostor verification attempts.

False Rejection: When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False Rejection Rate (FRR): The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The FRR may be estimated by FRR = NFR/NEIA or FRR = NFR/NEVA where:

- NFR is the number of false rejections.
- NEIA is the number of enrollee identification attempts.
- NEVA is the number of enrollee verification attempts.

ID-Based Authenticator/Identifier ("whom one is") – are characterized by uniqueness driver's license, passport, credit card, university diploma, etc., all belong in this category. So does a biometric, such as a fingerprint, eye scan, voiceprint, or signature. For both ID documents and biometrics, the dominant security defense is that they are difficult to copy or forge. However, if a biometric is compromised or a document is lost, they are not as easily replaceable as passwords or tokens (Newbold, 2008).

Identification/Identify: The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach seeks to find an identity amongst a database, rather than verify a claimed identity (Newbold, 2008).

Impostor: A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee.

Information Fusion: Consolidating information or evidence presented by multiple biometric sources (Ross et al.).

Knowledge-Based Authenticator ("what one knows"**)**: are characterized by secrecy or obscurity. This type includes the memorized password. It can also include information that is not so much secret as it is "obscure," or "secret from most people." Mother's maiden name and a favorite color are examples in this category. A security drawback of this type of authentication is that, each time it is shared for authentication, it becomes less secret.

Match/Matching: The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An 'accept' or 'reject' decision is then based upon whether this score exceeds the given threshold (Newbold, 2008).

Match Score Level Fusion: Multiple classifiers output a set of match scores that are fused to generate a single scalar score. As an example, the match scores generated by the user fingerprint images and the correct sequence entered may be combined via the simple sum rule in order to obtain a new match score which is then used to make the final decision (Jain, Flynn, & Ross, 2008).

Matching Score/Score: The level of similarity from comparing a biometric sample against a previously stored template (Newbold, 2008).

Minutiae: Specific points in a finger image consisting of ridge endings and bifurcations. Sometimes, other details, such as the points at which scars begin or terminate, are also considered. Minutiae vary from finger to finger and from person to person Bolle, Cornell, Pankanti, Ratha, and Senior, (2004).

Multi-Factor Authentication Method: When a user presents at least two different distinct pieces of evidence to identify who he/she is, such as something the user knows and something the user has (Hanche, Berti, & Hare, 2004).

Object-Based Authentication Method ("what one has"): are characterized by physical possession. Physical keys, called metal keys to distinguish them from cryptographic keys, are tokens that have stood the test of time well. A security drawback of a metal house key is that, if lost, it enables its finder to enter the house. This is why many digital tokens combine another factor, such as an associated password to protect a lost or stolen token. There is a distinct advantage of a physical object used as an authenticator; if lost, the owner sees evidence of this and can act accordingly.

Participant: A person taking part in the BIO-PIN Study.

Password Fatigue: A condition where users are overburdened with managing an increasing number of passwords to access different types of information (Dhamija & Dusseault, 2008).

Receiver Operating Characteristic (ROC): A graph showing how the false rejection rate and false acceptance rate vary according to the threshold.

Recognition: Alternative term for *identification*.

Reliability: Refers to the stability and consistency of the results (Creswell, 2008).

Template/Reference Template: Data representing the biometric measurement of an enrollee which used by a biometric system for comparison against subsequently submitted biometric samples (Newbold, 2008).

Threshold/Decision Threshold: The acceptance or rejection of biometric data is dependent on the match score falling above or below this threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application (Newbold, 2008).

User: A person engaged in operating the computer BIO-PIN™ application to authenticate to the computer system as part of the BIO-PIN™ Study.

Validity: Refers to how meaningful the results of the study are. It is important to make sure that survey instruments are reliable and valid (Creswell, 2008).

Verification/Verify: The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed to determine whether it matches the enrollees' template (Newbold, 2008).

Summary

The purpose of chapter one was to introduce the study, identify the research problem, discuss and identify any barriers and limitations to conducting this study, and to provide a theoretical basis for this study. The research problem addressed was that traditional user authentication methods, such as UN/PWs, still pose a significant vulnerability when accessing information systems. Valid literature supporting the need for this research was also presented. Chapter one also presented the main goal, specific goals, and specific research questions that were addressed during this study. The main goal of this research study was to examine the role of the authentication method (BIO-PIN™ versus the BIO+PIN versus UN/PW) and time on the effectiveness of authentication, as well as users' ability to remember BIO-PIN™ versus the BIO+PIN versus UN/PW. Prior literature that supports the main goal of this research was also presented (Furnell, 2007; Hayashi et al., 2008; Jain et al., 2006; Maty´aˇs & R´ıha 2010; Mujeye & Levy, 2013; Ross, 2007; Woodard & Flynn, 2005).

Chapter 2

Review of the Literature

The literature review covers prior research in the information security, information assurance, and biometric fields. This literature review serves as the foundation and justification for the research problem, research questions, and methodology. The major areas on which the research was focused on included biometrics, identification and authentication, information security access control methods, and Web-based access control methods. Authentication methods such as biometrics are increasingly being used in safety-critical applications such as nuclear power plants, aircraft, submarines, or medical devices, where the assurance of data protection is an issue of great importance (Jain, Hong, & Pantanti, 2000). Woodard and Flynn (2005) conducted a study on the three-dimensional (3D) finger surface and concluded that it is a viable choice as a biometric identifier for both authentication and identification; however, there is no known practical use of this approach being implemented today. Other areas covered included multi-biometrics, convenience of using password versus biometrics, and attack vectors.

In order for a human physiological or behavioral trait to serve as a *biometric characteristic* it must satisfy these four criteria: universality, uniqueness, permanence, and collectability (Jain et al., 2000; Prabhakar, Pankanti, & Jain, 2004):

- *Universality* refers to the criteria that all individual identifiers should possess as in human characteristic (five fingers on each hand, two eyes, arms, legs etc.).
- *Uniqueness* means that no two individuals should be identical in terms of their

identifier.

- *Permanence* means that the identifier should not change or be alterable (A behavioral biometric may evolve over time and physiological ones may still gradually alter with aging or other factors).
- *Collectability* means that the characteristic can be measured quantitatively.

For a biometric system to be practical, it must be accurate, fast, meet acceptability requirements, be harmless to the users, and accepted by the intended population. A biometric system must also be sufficiently robust to protect against various fraudulent methods and attacks.

Figure 2 shows a fingerprint with examples of a core, ridge bifurcations, and ridge endings that make up fingerprint minutiae points. According to Zhang (2004), as well as Bolle, Cornell, Pankanti, Ratha, and Senior, (2004), fingerprint minutiae are specific points in a finger image that take the shape of loops, arches, and whorls. Suna, Paulino, Feng, Chai, Tan, and Jain (2010) described fingerprints as the impression of friction skin on the finger. The main types of fingerprints are known as friction ridges, ridge endings, and bifurcations. Other details, such as the points where scars begin or terminate, on the fingers are also considered minutiae (Zhang, 2004). These points are used to distinguish one person from another. A study by Sun et al., (2010) found that, in most cases, fingerprints are unique enough to distinguish between identical twins; other methods, such as face and voice recognition, are not.

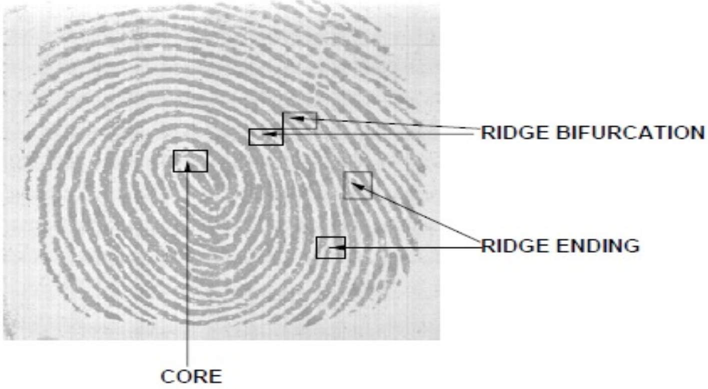


Figure 2. Fingerprint With Minutiae Points (Ross et al., 2003)

Bolle et al., (2004) observed that a clear and concise definition had not been developed for “minutiae.” They defined the term to acknowledge that the number and locations of minutiae may vary from finger to finger and person to person. When a set of finger images is obtained from an individual, the number of minutiae and the precise locations of the minutiae are recorded in the form of numerical coordinates for each finger. The results are usually entered and stored in a computer database, where they can be rapidly compared with other scanned finger images (Bolle et al., 2004).

A biometric system is a pattern recognition system that includes the software and hardware necessary for identifying an individual user as part of the authentication process. The process of acquiring and storing a pattern into the database is called biometric enrollment. To authenticate a user, a live biometric is captured using a scanner and it is converted into a template, which is matched with the stored template (Ross et al., 2006).

According to Jain et al., (2006), fingerprints are high in uniqueness and permanence, and medium in universality and collectability. Table 3 shows an example of how each of the biometric identifiers meets these criteria in varying degrees.

Table 3. Comparison of Biometric Identifiers (Prabhakar et al., 2004)

Biometric	Universality	Uniqueness	Permanence	Collectability
Fingerprint	Medium	High	High	Medium
Hand Geometry	Medium	Medium	Medium	High
Iris	High	High	High	Medium
Face	High	Low	Medium	High

The proliferation of information systems over the past decade has increased the demand for systems authentication. Although most information systems' authentication methods are UN/PW based, passwords still pose a significant limitation (Mujeye & Levy 2013, p. 122). The problems of traditional user authentication methods, such as UN/PW posing a significant vulnerability when accessing information systems, will continue until computer crime is eliminated or more effective methods of authentication are adopted by society (Furnell, 2007; Furnell, 2013). This vulnerability affects nearly all computer users, regardless of where they live or their demographics (such as gender, age, or computer skill level) (Furnell, 2007; Furnell, 2013). Stronger authentication using BIO-PIN™ may reduce fraud, identity theft, and the cost of managing and correcting those types of events.

User authentication has been practiced far longer than computers and telephones have been in existence. Intelligence and military organizations were among the first to practice authentication methods. For example, person 'A' would meet person 'B', and neither recognized the other by visual appearance. If person A and person B were spies, they would use some method of mutual authentication—from piecing together two halves of an object such as a either page torn in half, a small puzzle to exchange, or completing pre-arranged statements. Other methods in military history show couriers who delivered messages between different generals or political leaders and were not always recognized between military units. When facial recognition and/or voice recognition could not be proven in these situations, other methods to identify the couriers were developed.

The first method was passwords. For example, a bivouacked military unit might have established perimeter guards to provide security (Mallow, 2007). A courier might show up at any time and approach the guard, who would authenticate the courier by asking the courier for the password. This would have quickly provided authentication of the courier because only those within that army would have known the password. A general might provide the courier a ring or a seal (i.e. 'token'), known to all and unique to that general (Mallow, 2007). When the courier approached the camp perimeter, he would display the ring or seal to the guards to indicate that he came from the general and under his authority (Mallow, 2007).

Humans have used three methods of authentication throughout history; these methods continue to be:

- Something the person knows (the password).
- Something the person has (the general's ring or seal).
- Something the person is (face, voice, or fingerprints) (Menkus, 1998; Mallow, 2007).

According to Erilich and Zviran (2009), of the three categories "something the person knows" (knowledge-based authentication) is the most widely used method. Knowledge-based authentication can be further divided into three different categories:

- Question/answer-based.
- Character-based.
- Image-based.

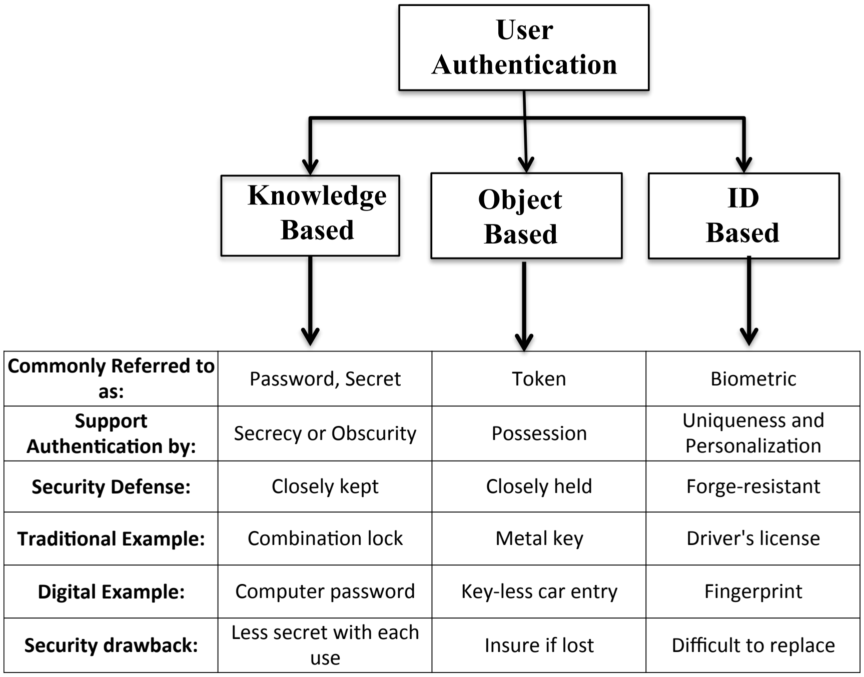
From these three categories, character-based authentication is still the most widely used. However, question and answer are sometimes used as a second means of validating who the user is A typical question might be something the user selects from a pull down window or creates such as a mother's maiden name, user's favorite color, or first car. Additionally, the CAPTCHA™ is used to validate the user is a human being and not a bot. It may be linked to the username on a per session basis. The personal security images alert the user they are on the appropriate Website based on an image they selected when the account was originally established or updated as a means of validating who the person is. An unsuspecting user might not know the correct image associated with the user account.

In order to implement an authentication system, there must be a reliable, repeatable standard that establishes immutable uniqueness of individuals. For example, in the past, the Bertillon system of bone measurements was used to identify prisoners (O'Gorman, 2003; Wayman, Jain, Maltoni & Maio, 2005). Henry Faulds, William Herschel, and Sir Francis Galton conducted quantitative identification through fingerprint and facial measurements in the 1880s (Wayman, et al., 2005). Digital signal processing techniques developed in the 1960s led immediately to work in automating human identification. Fingerprint recognition systems were among the first to be explored. This technology was applied to high-security access control, personal locks, and financial transactions (Wayman et al., 2005). The 1970s saw development and deployment of hand geometry systems. There was large-scale testing and increased government interest in the use of these "automated personal identification" technologies. Before the 1990s, forensic science depended on dental records, scars, and, tattoos (O'Gorman, 2003). According to Wayman et al. (2005) retinal and signature verification systems were developed in the 1980s and

1990s, followed by system development of facial and iris recognition in the 1990s.More recently, Deoxyribo-Nucleic Acid (DNA) in combination with fingerprints or other methods for definitive authentication (O’Gorman, 2003). All of these methods are repeatable standards that rely on unique physical characteristics of individuals as the primary factor of authentication (O’Gorman, 2003).

Passwords are the most prevalent form of authentication, but are only one of many technological methods available to secure systems from unauthorized access. Three modalities are typically considered in an authentication model: knowledge-based, object-based, and biometric-based (O’Gorman, 2003). Because the third identity methods do not depend on secrecy, biometrics is considered an identity authenticator much like a driver’s license number. A driver's license is not secret, but it's a good authenticator because it is paired with the individual's face and it is difficult to counterfeit (O’Gorman, 2003).

Different types of authentication methods can be combined to enhance security (see Figure 3). This is called *multi-factor authentication*. For security purposes, with a non-biometric method, each authenticator result must be satisfied; in effect a Boolean AND operation is performed for each factor’s authentication results, so all must be affirmative. A common example of multi-factor authentication is the bankcard. The combination of a bankcard and a password or PIN—two-factor authentication—is a better choice than a card alone because the card can be stolen and used. A card that is PIN-protected cannot be used without knowing the PIN (Weir, Douglas, Richardson, & Jack, 2009). This example of token plus password constitutes the vast majority of current multi-factor implementations. Generally, three-factor authentication has not been widely applied, although some high security applications may require it.



Commonly Referred to as:	Password, Secret	Token	Biometric
Support Authentication by:	Secrecy or Obscurity	Possession	Uniqueness and Personalization
Security Defense:	Closely kept	Closely held	Forge-resistant
Traditional Example:	Combination lock	Metal key	Driver's license
Digital Example:	Computer password	Key-less car entry	Fingerprint
Security drawback:	Less secret with each use	Insure if lost	Difficult to replace

Figure 3. Types of User Authentication Methods (O'Gorman, 2003)

Multi-biometric

Multi-biometric is defined as a system that consolidates the evidence presented by multiple biometric sources (Ross et al., 2006). For this reason, multi-biometric systems are considered more reliable than uni-biometric systems that use a single biometric in the authentication process. According to Ross (2006), multi-biometrics can help solve the problem of non-universality or insufficient population coverage and may effectively address the problem of noisy data. Noisy data is biometric data being presented to the system that has been contaminated due to imperfections or variations in the biometric (Jain et al., 2008). Multiple biometric sources also make it increasingly difficult for an impostor to spoof the biometric traits of a legitimately enrolled user.

According to Raja and Arumugaperumal (2013), another two-factor authentication method being used today is fingerprint matching and one-time mobile PIN number matching. This two-factor method is implemented when the user presents a fingerprint to the authentication server (first factor) and the authentication server responds by sending a text message or email to the user with a numerical PIN. The user then enters the numerical PIN for the second and final step in the two-factor authentication process. The biometric data required to establish this process is done during user initial registration to the system.

The BIO-PIN™ can be considered a multi-factor, multi-instance, and multi-sample system because it fits all those characteristics (Ross et al., 2006). According to Jain et al. (2008), *multi-instance* biometrics is defined as the use of the same type of raw biometric sample and processing on multiple instances of similar parts, such as two or more fingers or two irises. *Multi-instance* systems are often used to verify individuals enrolled in a very large database. Jain et al., (2008) also states that *multi-sample* biometrics include systems that acquire multiple samples of the same biometric trait collected during the enrollment and/or recognition phase (e.g. a number of fingerprint readings are taken from the same finger to ensure you have the best quality fingerprint).

The goal of this research study was to address the research problem by proposing a two-factor authentication method that is intrinsically bound to the user's biometric. The BIO-PIN™ may be easier to remember than some industry standard complex passwords or the BIO+PIN because users tend to forget passwords and PINs. Moreover, the BIO-PIN™ can be used in multiple accounts with little fear of being compromised, lost, or stolen because the biometric attribute being used for authentication is with the individual user at all times.

The knowledge base concerning biometric entering sequence was increased by having explored the BIO-PIN™ method for authentication as an alternative to current methods. By understanding that this method can be more effective, organizations can implement BIO-PIN™ or continue with traditional authentication methods. The potential for original work is where the BIO-PIN™ sequencing is used instead of a traditional PIN or biometrics by itself. Other methods, such as a biometric used in conjunction with a numerical PIN, have been investigated; however, vulnerabilities in using a numerical PIN exist. The numerical PIN can be guessed or obtained by launching a brute force attack against the PIN. This study did test the BIO+PIN to see how it related to the effectiveness and/or differences compared with the BIO-PIN™ sequencing method.

There are 10,000 possible four digit PIN numbers or codes. According to DataGenetics (2012), the PIN most often used can be interpreted as years, e.g. 1935, 1954, 1967, and so on. It appears that many people use a birth year or (possibly) an anniversary year as their PIN. This makes the PIN easier to remember but it also increases the predictability. Other PINs are formed by patterns or sequences, the top 20 PIN numbers and the frequency of their use is listed in the Table 4. The number one PIN is 1234 and it was selected 10.71 percent of the time. Another of the more popular four digit numbers is 2580, straight down the middle of the telephone dial pad. Likewise, PINs that were least likely to be used were 8068, 8093, and 9629. They are spread across the computer keyboard number row and are awkward to select. Hackers will try the most popular PINs first when attacking your credentials. For the BIO-PIN™ study, users were asked to create a PIN that was never used before but most likely they followed a similar approach to creating the PIN as part of the BIO+PIN.

Table 4. Most Popular PINs and Frequency of Use (DataGenetics, 2012)

Ranking No.	PIN	Frequency of use
#1	1234	10.71%
#2	1111	6.02%
#3	0000	1.88%
#4	1212	1.20%
#5	7777	0.75%
#6	1004	0.62%
#7	2000	0.61%
#8	4444	0.53%
#9	2222	0.52%
#10	6969	0.51%
#11	9999	0.45%
#12	3333	0.42%
#13	5555	0.40%
#14	6666	0.39%
#15	1122	0.37%
#16	1313	0.30%
#17	8888	0.30%
#18	4321	0.29%
#19	2001	0.29%
#20	1010	0.29%

Attack Vectors

Although fingerprint biometrics have numerous advantages, authentication systems are still vulnerable to a variety of attacks. Ratha et al., (2001) analyzed these attacks and grouped them into eight classes. Figure 5 shows these attacks along with the components of a typical biometric system that can be compromised. Fake biometric (Type 1) uses synthetic fingerprint, face, or iris to spoof the system. Matsumoto, Matsumoto, Yamada, and Hoshino (2002) used artificially created gummy (gelatin) fingers to successfully attack 11 different fingerprint verification systems with an acceptance rate between 67% and 100%. These results introduced the need for software that could determine the temperature and connectivity for fingerprint "aliveness" detection. The aliveness detection capability was added to other modalities such as iris, retina, and facial recognition.

According to Uludag and Jain (2004), in a *replay attack* (Type 2) the biometrics are intercepted or captured and replayed to the authentication system. The feature extractor module (Type 3) is compromised to produce feature values selected by the attacker. Genuine feature values are replaced (Type 4) with the ones selected by the attacker. The matcher can be modified to output an artificially high matching score in attack Type 5. Type 6 uses reverse engineering to reconstruct the minutiae in the database in order to attempt a *masquerading* attack. The attack on the template database can include adding, modifying, or removing templates from the database. To counter this attack, the raw biometric templates may need to be secured using encryption, checksum, or hashing techniques (Uludag & Jain, 2004). The transmission medium between the template database and matcher may be an attack point for Type 7, resulting in the alteration of the transmitted templates. Finally, with the Type 8 vulnerability, the attacker may be capable of overriding the matcher results (accept or reject) (Uludag & Jain, 2004).

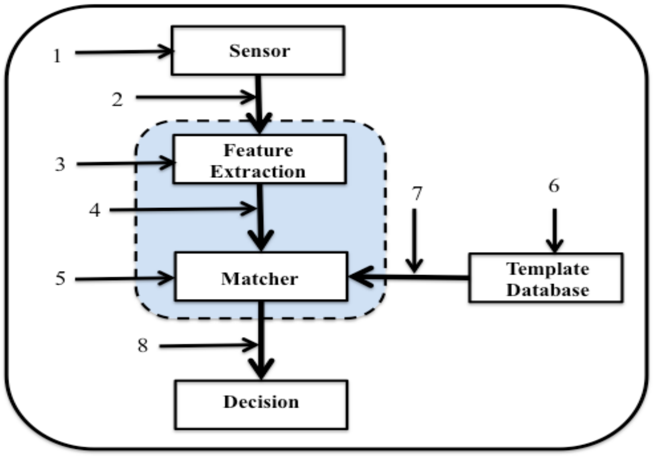


Figure 4. Attack Points in a Biometric Authentication System (Uludag & Jain, 2004)

Schneier (1999) compared traditional security systems with biometric systems. He concluded that the lack of secrecy (e.g., leaving fingerprint impressions on the surfaces we touch) and non-replaceability of biometrics (e.g., once the data is compromised), are major concerns with biometric systems. He also noted the concern that there is no way to return to a secure situation, unlike replacing keys or passwords. In *contamination (covert acquisition),* an attacker can surreptitiously obtain biometric data of legitimate users (e.g., lifting a latent fingerprint and constructing a three-dimensional mold) and use it to access the system. Maltoni, Maio, Jain, and Prabhakar (2003) describe typical threats for a generic authentication application such as a *Denial of Service (DoS),* where an attacker corrupts or ties up the authentication system so that legitimate users cannot use it. In insider threats such as in *collusion*, a legitimate privileged user (e.g., system administrator) is the attacker who illegally modifies the system (Maltoni et al., 2003). In *coercion*, attackers force the legitimate users to access the system (e.g., using a fingerprint to access ATM accounts under duress or threat of physical harm). Although no authentication method or information system is bullet proof, managing risk to an acceptable level is still the main goal. Based on all the various types of attacks and countermeasures found in the literature, the BIO-PIN™ concept of something the user is and knows could be added to the list of countermeasures for certain types of attacks.

Convenience

Traditional knowledge-based or token-based personal identification or verification systems are tedious, time consuming, inefficient, and expensive (Zhang, 2004; Weir, et al., 2009). Knowledge-based approaches use something the user knows, such as a password or

PIN for personal identification; token-based approaches use something the user has, such as a secure ID, passport, credit card, or driver's license. Tokens are time consuming and expensive to replace and passwords are hard to remember (Zhang, 2004; Weir et al., 2009).

Table 5. Security Advantage of Combining Authenticators (O'Gorman, 2003)

Authenticator Combination	Security Advantage	Convenience Drawback	Example
Knowledge- and Object Based	Lost/stolen token protected by password	Must carry token and memorize password	PIN-enabled bank card
Object- and ID-based	Lost-stolen token protected by ID	Must carry token but not ID if it is a biometric	Photo-ID
Knowledge and ID-based	Two factors provide security in case either is compromised	Have to memorize password and have ID	Password and biometric for computer access
Knowledge-, Object-, and ID-Based	A third factor to provide security in case two other factors are compromised	Have to memorize password, carry token and have ID	Military applications requiring photo-ID checked by guard, plus password

A combination of UN/PW or PIN is commonly used to authenticate to information systems (Ratha, Connell, & Bolle, 2001). A dictionary attack is a malicious event where an attacker builds a database populated with various combinations of possible passwords (referred to as the "dictionary") and tries all possible combinations until one works (Vykopal, Plesnik, & Minarik, 2009).

According to O'Gorman (2003), if an authenticator is inconvenient, it may not be used or used correctly, which may make it vulnerable to compromise. Users who must remember multiple, changing passwords are notorious for password mishaps. Although tokens can reduce the problem of remembering passwords, the user must remember to carry the token. Biometrics alleviates the problem of forgetting the token and/or passwords but some users may experience the inconvenience of false non-match results. For biometrics and tokens being used in a networked environment, there are other convenience issues such as how best to register/enroll, renew, recover, and revoke the authenticator. Since a token is an object, it must be put into the hands of the authorized person either personally or by delivery. Correspondingly, it may need to be removed from the user if authorization is revoked.

In spite of the many criticisms of passwords, such as that they are easy to crack, poorly constructed, and easy to compromise or forget, they still appear to remain the de facto approach to user authentication (Furnell, 2007). They are used in the vast majority of situations because of their convenience, familiarity, and universality in cross-device applications (Furnell, 2007). There have been many attempts to solve the password problem such as increasing the number of characters in the industry standard complex password from eight to 12, and in some cases 14. The password is strengthened but the users still may have trouble remembering such lengthy passwords as already discussed by Dhamija and Dusseault (2008). These attempts were somewhat unsuccessful because users did not remember the passwords and typically wrote them down, which made them subject to compromise. Anyone who could gain access to the password could potentially impersonate the authorized user.

It appears that without an easy to remember, yet strong, authentication method, society will continue to use the same traditional authentication methods. Users have traditionally used poor password choices, created weak passwords, written down the passwords, and/or used the same password for multiple systems for indefinite periods of time (Furnell, 2007). If the process goes unchanged it may not evolve to what may be a more effective approach, and users will live with the same criticisms.

Password policies dictate the minimum number of characters, complexity, expiration and/or the number of times a user can reuse the same password. The trend has been to lengthen the password and increase the complexity in order to strengthen it (Furnell, 2007). This may eventually cause the system to be more vulnerable as users write down passwords or store them in convenient places because they have a hard time remembering industry standard complex passwords. This could lead to compromise passwords (Dhamija & Disseault, 2008; Mujeye & Levy, 2013).

Summary

The main contributions of this study are to advance the understanding of users' authentication to information systems, security threats, problems with user authentication, personal information sharing habits, and information sharing practices. Information gained from this study may help organizations develop better approaches to securing their users' personal information as well as the organization's information. Success in this area includes, implementing security training and awareness programs where users are trained to recognize weaknesses in their current authentication methods, and be exposed to and more accepting of other methods of authentication that may prove to be more secure. Moreover, implementation of information security policy that addresses these types of access control and authentication concerns may lead to a reduction in the occurrence of identity theft.

Chapter 3

Methodology

Overview of Research Methodology/Design

This research study used a quasi-experimental multiple baseline design method to evaluate the effectiveness of the BIO-PIN™ in the research questions. A quasi-experiment has treatment, outcome measures, and experimental units that do not use random assignment to assign participants to the control or treatment group (Cook & Campbell, 1979). It depends on non-experimental groups that differ from each other in many ways other than the way the treatments are being tested (Cook & Campbell, 1979). The multiple-baseline design is based on a robust longitudinal approach, where the participants are engaged in the treatment for a longer duration (Levy & Ellis, 2011). This study engaged participants for a 10-week period.

Research Design

The need for further study in this topic is the result of observations in the way biometric attributes are used in industry today. The 2009 International Biometric Conference in Tampa, Florida, focused primarily on biometrics for identity management, crime, and border security. It appeared that little attention was given to biometrics as a significant type of access control to computer systems or widespread use as a multi-factor authentication method. Literature review and research shows that users are frustrated with the continuing increase in password length (from eight characters to 14 characters in some cases), frequent password changes or expiration periods, as well as trying to remember multiple complex industry standard passwords to access different systems (Furnell 2007 & 2011). A number of previous researchers and investigators have expressed the need for further investigation into authentication methods for similar reasons (Gaw & Felten, 2006; Halderman et al., 2005; Ives et al., 2004; Sasse et al., 2001). After reviewing several studies and peer-reviewed papers, it was apparent that there was additional work in this area to complete.

The research design in this study was conducted by using a commercial fingerprint scanner that captured the digital images of the users' fingerprints, then verified and stored those images in the access database on a standalone computer. Each user was asked to select a BIO-PIN™ sequence consisting of four fingerprints in a specific order and a BIO+PIN consisting of four fingerprints and a 4-digit numerical PIN for the BIO+PIN account. For identity verification, each user presented their BIO-PIN™ and BIO+PIN to the fingerprint scanner device. If during the user authentication session a failure-to-acquire error on a specific finger occurred, that finger was repeated to ensure all fingerprint minutiae was sufficiently captured. The BIO-PIN™ sequence was validated against the enrolled template of the user's fingerprint sequence. The computed feature vector was compared with the retrieved template to compute a matching score. This matching score was compared with a preset threshold value where the subject's identity was verified. After each successful attempt to enter the correct sequence (initiated at each test interval) the user was authenticated. The user then accessed the Internet through the BIO-PIN™ website and sent an email to the Principal Investigator (PI) to complete a session.

Figure 6 illustrates the BIO-PIN™ enrollment, identification, and authentication process. User fingerprints were collected and stored in the database. The user was enrolled and the BIO-PIN™ sequence established. The user's BIO-PIN™ was tested against the stored fingerprints and sequence to ensure it authenticated the user and a valid account was created. Once the user account was activated, the user attempted to access the information system by entering the username and BIO-PIN™. The biometric authenticator searched the database for the correct fingerprint image and validated the fingerprint images and that the proper sequence was entered. If the fingerprint and the sequence both met the established pre-determined threshold (>70%), the user was granted access to the information system. The pre-determined threshold of 70% is the percentage of the probability of assurance that the user was the person attempting to authenticate to the system. After validating that three of the four fingerprints were entered in the correct sequence, there was at least 70% assurance that this user was who they claimed to be. The user did not have knowledge of the percent or threshold for authentication, only the authentication system.

The login successes and failures from each session using each authentication method was collected and documented in the BIO-PIN™ Participant Information Log. The study captured the participants' age, gender, years of computer use experience, and number of accounts. Additionally, an account was created using the captured digital fingerprint images of the users fingerprints for the BIO+PIN—four fingerprints in no particular order and a 4-digit numerical PIN. In this instance, each user was asked to create a 4-digit numerical PIN. For identity verification using BIO+PIN, users entered their four fingerprints into the biometric scanner and then their 4-digit numerical PIN from the computer keyboard into the BIO+PIN application screen displayed on the computer.

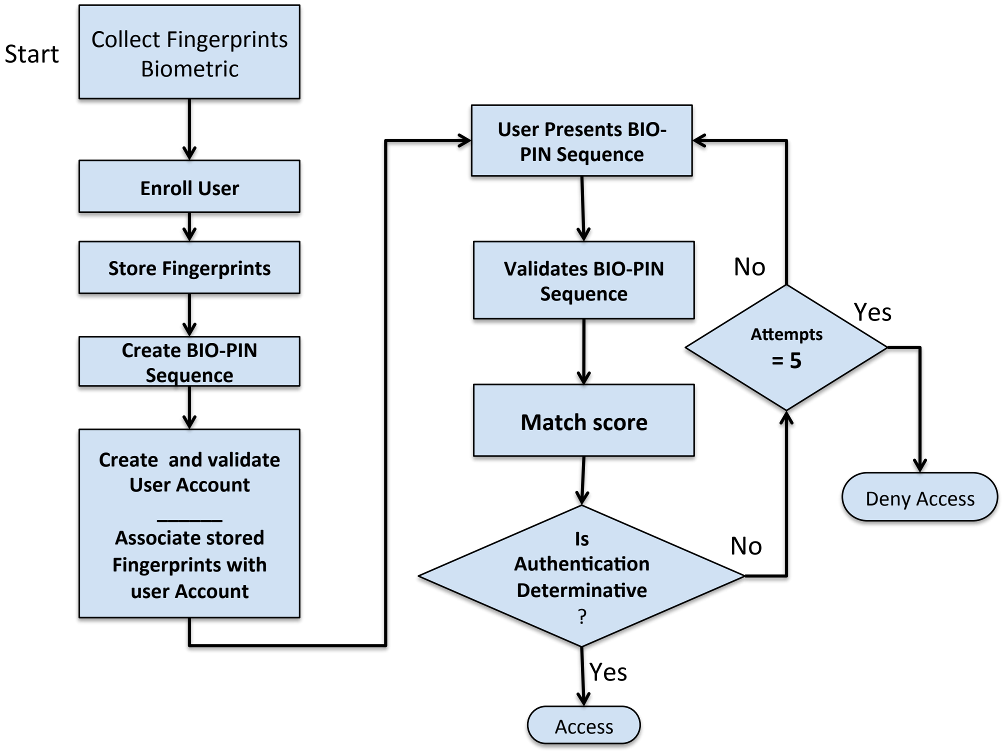

Start
Collect Fingerprints Biometric
Enroll User
Store Fingerprints
Create BIO-PIN Sequence
Create and validate User Account
Associate stored Fingerprints with user Account
User Presents BIO-PIN Sequence
Validates BIO-PIN Sequence
Match score
Is Authentication Determinative ?
Yes
Access
No
Attempts = 5
No
Yes
Deny Access

Figure 5. BIO-PIN™ Enrollment, Identification, and Authentication Process

Participant (User) Authentication Activities

Participants were registered by selecting a username from one of the names of the 50 United States, 50 state capitals, or major cities within the 50 states. The user name was required to be at least eight characters long. When the selected username was less than eight characters, additional alpha-numeric characters were added to make up the difference (i.e., utah0815, Topeka11, or albanyny). Next, the user created an industry standard, complex password of eight or more characters consisting of at least one capital letter, one number, and one special character, and then validated the password. Next, all five fingerprints from one of the user's hands was presented to the fingerprint reader several times until an acceptable image of each fingerprint was captured. For the third authentication method, the users created a BIO+PIN by selecting four fingerprints and a 4-digit numerical PIN. The BIO-PIN™ application was closed and reopened after each user enrollment process was completed to finalize the account creation/registration process. This step also reset the device and application for the next user to register to eliminate any possible errors.

For identity verification during subsequent validation sessions, the users entered their BIO-PIN™, UN/PW, and BIO+PIN into the BIO-PIN™ Application. After successfully entering the correct sequence for each method, the user was logged in. Each login attempt was recorded as either an "S" for success or an "F" for failure. The failure designator "F" was added for each failed attempt. For example, if there were three failed attempts, three "F"s were recorded (FFF). When the user was successful in the login attempt, the success designator "S" was recorded. The log would record "FFFS" if there were three failed attempts before the user was successful. The total number of unsuccessful login attempts allowed for each of the authentication methods was five (recorded as FFFFF). After all the login attempts were completed, the user session was connected to the BIO-PIN™ Study Web-page through a link on the BIO-PIN™ Study application. The user sent an email to the PI from the "contact us" page with an appropriate message using the provided return email address. The user activities were observed by the PI and recorded in the sample BIO-PIN™ User Information Log (data collection).

User’s Ability To Remember Credentials

The participant’s ability to remember their credentials was calculated based on the number of successful attempts (S) and number of failed attempts (F). Each attempt is counted and accumulated until the user was successful or reached a number of five failed attempts. Table 6 illustrates how these attempts were accounted for. Success or failure was counted by counting the number of failed attempts (F) and assigning them a number ranging from 0 to 5 based on the total number of failed attempts during this study. The lower the number of attempts the more successful the participant was in remembering their credentials and accessing the BIO-PIN™ Study website.

Table 6. Success, Failure, and FRR

Success (S) / Failure (F)	User Ability	False Rejections	Weight
S	S	0 FR	0
F	1F+S	1FR+S	1
FF	2F+S	2FR+S	2
FFF	3F+S	3FR+S	3
FFFF	4F+S	4FR+S	4
FFFFF	5F	5FR	5

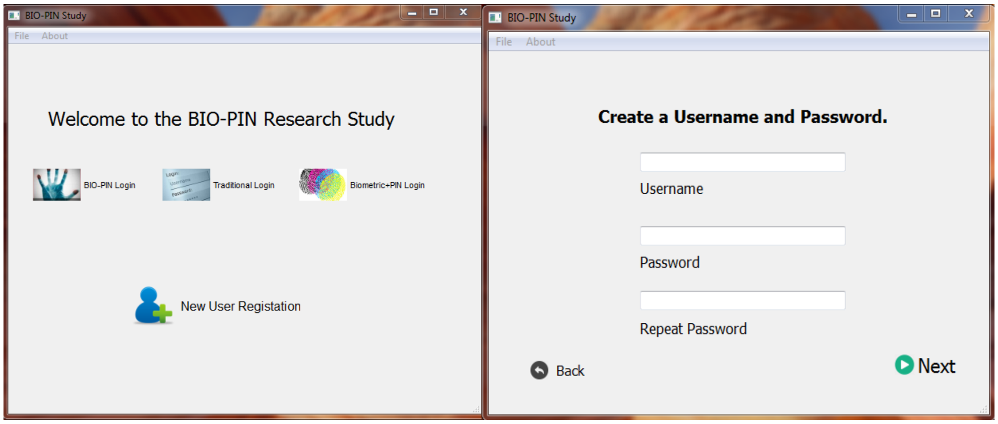
Authentication Effectiveness

The number of False Rejections (FR) was similarly counted, however it was based on the number of times a legitimate participant’s fingerprints were falsely rejected. The number of false rejects were counted and accumulated until the user was successful or reached a number of five false rejections. Table 6 illustrates how these false rejections were accounted for during this study. FR were counted incrementally each time the BIO-PIN™ application failed to recognize the fingerprints when presented in the correct order and assigning a number ranging from 0 to 5 based on the total number of false rejections. The lower the number of attempts represents a lower FR.

The FR only applied to the BIO-PIN™ authentication method. The username and password authentication method does not use a fingerprint as part of its authenticator. The BIO+PIN authentication method used fingerprints in any order and a numerical PIN; however, the emphasis for granting access is weighted more on the PIN which must be an exact match while fingerprints can be entered in any order and isn't as heavily weighted for authentication using that method.

Based on the username assignment, each user started the authentication process using a different method. Those users whose username was one of the 50 states started each session logging in with the BIO-PIN™ first. Those who had state capital usernames started each session with UN/PW and, finally, those with major cities started each session with the BIO+PIN. By randomly authenticating with a different method, the study tried to eliminate any bias in the authentication process by having every user login in the same way each time. The account creation, login attempts, and fingerprint scanned successes and failures were all recorded on a hard copy of the spreadsheet and transcribed to an electronic excel spreadsheet.

Figure 6 is the first in a series of screen shots of the BIO-PIN™ application as the user progressed through the login session using the application from registration to login attempts. It shows the application homepage where users accessed one of the three authentication methods and the account creation page where users entered their username and password for the study. The right side of Figure 6 shows the username and password creation Graphical User Interface (GUI).

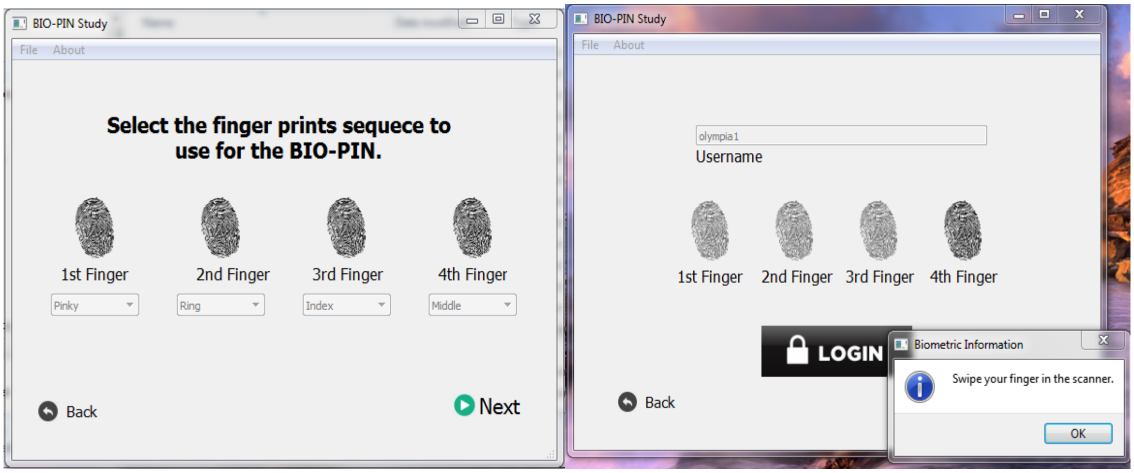


Welcome to the BIO-PIN Research Study

Create a Username and Password.

Figure 6. BIO-PIN$^{™}$ Application Welcome and Accounts Creation Screen-shots

Figure 7 has screen shots of the BIO-PIN$^{™}$ Study Application fingerprint scan and sequence selection page. The page on the left depicts the scanned fingers and the selection sequence for the BIO-PIN$^{™}$. A drop down list allowed the users to select which fingerprints would be used for the sequence by designating any four of the five fingers. The right side shows the light gray and dark gray fingerprints as the user progressed through authentication. Light gray depicted fingerprints that had been swiped and the dark gray depicted fingerprints that remained to be swiped. The popup window alerted the user to swipe each finger.



Select the finger prints sequece to use for the BIO-PIN.

1st Finger: Pinky
2nd Finger: Ring
3rd Finger: Index
4th Finger: Middle

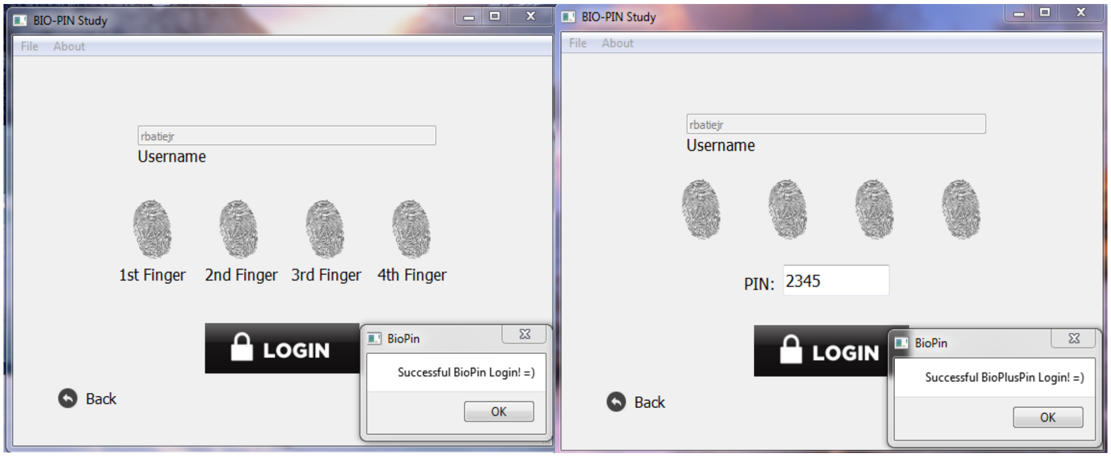
Username: olympia1

Biometric Information

Swipe your finger in the scanner.

Figure 7. BIO-PIN$^{™}$ Application Fingerprint Sequence Screen-shot

Figure 8 has screen shots of the BIO-PIN™ Study Application that included the correct username and successful login with the BIO-PIN™ sequence. The page on the right shows the successful login of the BIO+PIN with the numerical PIN number.



Username: rbatiejr

Successful BioPin Login! =)

Username: rbatiejr

PIN: 2345

Successful BioPlusPin Login! =)

Figure 8. BIO-PIN™ Fingerprint Sequence and BIO+PIN Successful Screen-shots

Demographics and Data Collection

Table 7 shows the form created to collect the demographic data on the study participants. It includes details on gender, age group, number of accounts, and frequency of IT usage. This data was collected from each user and added to the Excel spreadsheet. The data recorded in the spreadsheet was transferred into the Statistical Package for the Social Sciences (SPSS) for comprehensive statistical analysis and management for the final report.

Participants were asked to provide the information in Table 7 as part of the registration process. Additionally, three questions were asked:

(1) How does the user create their passwords?

(2) What method does the user use to remember their password?

(3) At the completion of the study, which authentication method do they feel was easiest to remember?

Table 7. User Registration and Data Collection Form

BIO-PIN Study Participant Data Collection

Participants Identification/username	**US State**	**State Capitol**	**Or**	**Major City**
Gender:	**M**	**F**		
Age Group	**18-30**	**31-35**	**36-50**	**51-55**
	56+			
Number of Computer/ Internet accounts	**0-5**	**6-10**	**11-15**	**16 +**
Frequency of computer/ Internet use	**5-8 hours per day**	**2-4 hours per day**	**1-5 hours per week**	

Measures

Salkind (2009) discussed and defined three components of measurement reliability. This study used the *true score* (or the perfect score) in the case of user authentication. True score was measured using the algorithm described when all user inputs were correct and the numerical value equaled 100%. The threshold is the score where the user was granted access based on the input of the correct UN/PW (yes or no), BIO+PIN, (fingerprints + numerical PIN), or BIO-PIN™ sequence when the sequence entered met a minimum pre-determined score (>70%). This arbitrary setting was based on the algorithm example discussed in the section titled BIO-PIN™ Algorithm Operations Example. A match score greater than 70% or .70 represents the assurance that the user was the person attempting to authenticate to the system. The BIO-PIN™ algorithm operations and the BIO+PIN algorithm operations examples discusses how the users authenticated using this process; and how the relationship between false-matched, false-accept, and error-in-sequence were captured for a single authentication scoring.

BIO-PIN™ Algorithm Operations Example

The example in this section is of a linear algorithm where the BIO-PIN™ sequence had a threshold of greater than 0.70 (this value is provided as an example and it could vary based on other factors) for acceptance and each fingerprint had a weighted value. The BIO-PIN™ authentication process was evaluated according to the following algorithm:

R= Recognition, S = Sequence, and w = weighting factor

$R \cdot w_r + S \cdot w_s > 0.70 \mid w_r = 0.3; w_s = 0.70$

Where $w_r + w_s = 1$ and R corresponds to a total percentage value corresponding to correct biometric readings, and S corresponds to a total percentage value corresponding to presenting the fingerprint in the correct sequence. The fingerprint and the knowledge of the sequence were fused together to establish the authentication. In this example, the user presented his/her fingerprints:

Biometric parameters: four fingers (1, 2, 3, and 5)
Stored Sequence: 5+2+1+3
Entered Sequence: 5+2+4+3
Each biometric reader: 5=accept, 2=accept, 4=reject, and 3= accept

Which resulted in:

R = 25% + 25% + 0% (erroneous reading) + 25% = 75% or 0.75

S = 25% + 25% + 0% (not in sequence) + 25% = 75% or .75

Thus, $R \cdot w_r + S \cdot w_s = (.75 \cdot .70) + (.75 \cdot .30) = .525 + .225 = .750$

As 0.750 is more than the overall predetermined threshold of 0.70, this user was authenticated. This approach helps to compensate for any anomalies that might happen with the fingerprint readers that give errors such as a dirty reader or failure to acquire. These anomalies have traditionally been a problem and have generated numerous user complaints (particularly for earlier model fingerprint readers). This approach is similar to the way a credit card company may track the buying habits of cardholders: the company becomes familiar with where the cardholder shops, how much the cardholder spends on average at each merchant, and the types of products the cardholder buys. Although this example illustrates a cardholder's buying habits it also is an indication that this buyer is the authorized user based on their buying habits. When the cardholder does something out of the ordinary the credit card company is alerted of possible fraud.

In another example, the user attempted to access the system, but presented a fingerprint sequence that had erroneous readings due to memory or false rejection and resulted in denial of access:

> Biometric parameters: four fingers (1, 2, 3, & 5)
> Stored Sequence: 5+2+1+3
> Entered Sequence: 5+2+4+1
> Each biometric reader: 5=accept, 2=accept, 4=reject, and 1= reject (FRR)
> R = 25% + 25% + 0% (erroneous reading) + 0% (erroneous reading) = 50% or 0.50
>
> S = 25% + 25% + 0% (not in sequence) + 0% (not in sequence) = 50% or 0.50
>
> Thus, $R \cdot w_r + S \cdot w_s = (.75 \cdot .70) + (.50 \cdot .30) = .525 + .150 = .675$

As 0.675 is less than the overall predetermined threshold of 0.70, this user attempt was not authenticated.

BIO+PIN Algorithm Operations Examples

In this example is where the "BIO" (fingerprints) "+PIN" (a four-digit numerical sequence) is much like the UN/PW: it is either all or nothing. The combination of four randomly entered fingerprints plus the 4-digit numerical PIN sequence must be complete and accurate or the user will not be granted access to the information system. The BIO+PIN authentication process was evaluated according to the following algorithm:

R= Recognition and NS = Numerical PIN Sequence

R + NS = 1

R corresponds to a total percentage value corresponding to correct biometric readings, and NS corresponds to a total percentage value corresponding to presenting the 4-digit numerical PIN in the correct sequence. The fingerprint and the knowledge of the 4-digit numerical sequence were fused together to establish the authentication. In this example, the user presented his/her fingerprints plus the 4-digit numerical PIN sequence:

Biometric parameters: four fingers (1, 2, 3, & 4) in any order
Each biometric reader: 4=accept, 3=accept, 2=accept, and 1= accept
Plus
Stored 4-digit Numerical PIN Sequence: 0+8+2+3
Entered 4-digit Numerical PIN Sequence: 0+8+2+3

The four fingerprints were presented and accepted; however, there was no particular order in which they needed to be presented. Additionally, any one of the four fingerprints may be rejected due to the potential for false or inaccurate reading of the fingerprints presented. As the user's four fingerprints were recognized and the user entered the numerical PIN in the correct sequence, this user was authenticated.

In this example, the user attempted to access the system, but presented fingerprints plus the 4-digit numerical PIN sequence that had erroneous readings and resulted in denial of access:

> Biometric parameters: four fingers (1, 2, 3, & 4) in any order
> Each biometric reader: 4=accept, 3=accept, 2=reject, and 1= reject
> Plus
> Stored 4-digit Numerical PIN Sequence: 0+8+2+3
> Entered 4-digit Numerical PIN Sequence: 0+8+3+2

As the user did not enter the PIN sequence in the correct order, this user was not authenticated and was denied access.

Study Environment

To ensure this study was reliable and that threats to data accuracy were reduced, the following measures were taken.

- The study was conducted in a general office environment (or residence) with low noise and adequate lighting so the participant would be comfortable and less distracted.
- All aspects of the study were documented to include date and time of day the sessions were held (between 9:30am and 5pm on specific dates over 2-, 3-, and 4-week intervals).
- The number of times the participant logged in correctly or incorrectly using each authentication method was recorded in the spreadsheet (i.e., *true score).*

Each participant was measured based on the number of successful authentication attempts and established controls for age, gender, frequency of IT usage, and number of accounts.

In the dissertation, two-factor authentication is something the user has (fingerprints) and knows (knowledge of the correct sequence). Users were required to remember either the biometric sequence of fingerprints entered in the case of the BIO-PIN™ or a 4-digit numerical PIN in the case of BIO+PIN. The fingerprint quality and sensitivity of the fingerprint reader reduced the false rejection or failure-to-acquire rates. This was verified during preliminary testing of the device and authentication process.

Reliability and Validity

It was important to make sure that the quasi-experiment was reliable and valid. *Reliability* refers to the stability and consistency of the results (Creswell, 2008). A study is considered highly reliable, if other researchers can replicate it and obtain similar results (Gummesson, 2007). *Validity* refers to how meaningful the results of the study are (Creswell, 2008).

Internal validity

Internal validity refers to the quality of the research measures, the control of the variables being studied, and the meaningfulness of the results (Levy & Ellis, 2009). Internal validity refers to the assurances that the measured variables were indeed the measures of the phenomena. There were multiple factors that posed a threat to the internal validity of the study. Users generating familiar passwords posed the greatest internal validity threat to this study, because users routinely choose easy to remember or easy to guess passwords, they also choose passwords that are very familiar to them (Ratha et al., 2001). To minimize the threats to internal validity, the users were asked to create a totally new password that was consistent with the industry standard complexity and that they had never used before. That password was documented and kept confidential from all participants. Other possible internal threats with this study were that the software or the biometric apparatus could malfunction, or participants could have a change of heart and opt-out during the course of the study. To mitigate these threats, the application was tested first to ensure it functioned properly and that backup hardware and software was made available in case of failure. Finally, participants were trained on the proper use and methods as part of the briefing on the study and the importance of their participation.

External validity

External validity refers to the generalization of the results to other studies (Steckler & McLeroy, 2008). External validity uses statistical generalization to extrapolate the research beyond the immediate form of inquiry (Riege, 2003). This study used the quota sampling strategy to manage an acceptable participant sample size. The study looked for trends in the data collected to understand how the users' engagement differed from one another based on their demographic indicators. Generalizing the results of their engagement mitigated the risks to external validity.

Sample

This study used a quota sampling strategy for the participants. Quota sampling is used when elements of the strata are present and stratified sampling is not possible. Quota sampling ensures that, to some degree, all the population in the strata is represented. The problem with this strategy is that the degree of generalizability may be questionable (Salkind, 2009). The quota sampling size this study used was 47 participants of varying ages, gender, frequency of IT usage, and number of computer accounts. Since this is a quota sampling, the response rate was monitored to account for all individuals who were asked to participate whether or not they accepted the invitation.

Data Screening

Pre-analysis data screening involves a process of detecting and dealing with irregularities or problems with data collection (Levy, 2006). Pre-analysis data screening was performed to ensure consistency and accuracy of the data. Data must be evaluated for accuracy and consistency to ensure the results are valid (Mertler & Vanatta, 2010). According to Mertler and Vanatta (2010), the four primary reasons to conduct pre-analysis data screening are to:

1) Ensure accuracy of the data collected.

2) Address the issue of response-set.

3) Address the issue of missing data.

4) Address the extreme cases, or outliers.

This study took the necessary steps to address data accuracy by documenting the participant's response during the quasi-experiment and recording the results immediately after the actions had been completed. Given that this study was not survey-based, the issue response-set was irrelevant. According to Levy (2013), missing or erroneous data may be attributed to typos or data entry errors. Extreme cases or outliers were further analyzed and evaluated to determine if they were an anomaly caused by a flaw in the data collection or analysis process. The data was documented in the multivariate data matrix as the experiments were conducted. The data was transferred from the hardcopy multivariate data matrix to an electronic spreadsheet version (Microsoft Excel). The multivariate data matrix was developed from the excel spreadsheet and contained various types of data collected on each test case participating in this study. All login attempts by the participants were captured in the BIO-PIN™ application audit logs. The PI reviewed the data generated by this study to ensure any errors were caught prior to final data entry and analysis. The BIO-PIN™ application audit logs were reviewed and analyzed to validate how many successes or failures each user had before being granted access to the information systems. The number of successes or failures was based on the users ability to remember BIO-PIN™ sequence, entering the correct numerical PIN for BIO+PIN and entering the correct UN/PW.

To satisfy the pre-analysis data collection and screening the PI personally registered each user and ensured their BIO-PIN™ study accounts worked properly as indicated by the successful registration logs. After registration was complete the PI observed every login attempt during each subsequent login session of the BIO-PIN™ Study over the 10-week period. Each user was instructed on which authentication method they would use first in their login attempts based on the type of username they chose. If their username was a state, they started with the BIO-PIN™ method; if their username was a state capital, they started with UN/PW; if their username was a major city, they begin the login session with the BIO+PIN method. Each authentication attempt was observed and recorded as either a success or failure (Successful/Unsuccessful) per the application logs. At the conclusion of the session the user was verbally notified with the number of successes and/or failures as a result of their login attempts they had during the session. Users were encouraged if they had difficulties remembering their authenticators and complimented if they were successful. At the completion of the login sessions, the PI immediately and carefully entered the results into the excel spreadsheet.

Each user's BIO-PIN™ application audit logs and the results were reviewed against the excel spreadsheet. The application log is the electronic record that shows the true number of successful or failed login attempts. The participant's success rate logging into the BIO-PIN™ application with UN/PW, BIO-PIN™ sequence and BIO+PIN was used to determine how well they remembered the authenticators. The registration logs serve as the baseline and show only the successful registration of each user with the three authentication methods. In each case the final result was a successful login with each method and serves as completed registration. After review of the excel spreadsheets and the application logs, there appears to be no missing data or outliers in the data collected. Based on the criteria of Mertler and Vanatta (2010), no other pre-analysis was warranted for the BIO-PIN™ Study.

Data Analysis

This section will address how each of the Research Questions and Hypotheses in this study was addressed. Hayashi et al., (2008) conducted a study where users authenticated by selecting a series of pictures in a sequence, as something the user knows. Woodard and Flynn (2005) conducted experiments on 3D finger surface over a set period of time using several experimental groups and multiple modalities. The experiments demonstrated that a biometric system that utilizes multiple modalities can achieve better performance. The combination of the characteristics of finger surface (or fingerprint) data with other biometric identifiers such as face, ear, or iris patterns for example, could result in higher verification rates. This study builds on these previously researched approaches to address the research questions and hypotheses presented here.

Addressing the Research Questions

The study used descriptive statistics, mean and standard deviation to analyze some of the demographic results. The independent, dependent, and control variables of the research questions were addressed using the Multivariate Analysis of Variance (MANOVA) statistical analysis to compare BIO-PIN™ versus UN/PW versus BIO+PIN authentication methods throughout this study for RQ1 thru RQ3. To assess the relationships noted for age, gender, user experience, and number of accounts, Multivariate Analysis of Covariance (MANCOVA) was used to address RQ4 (Cook & Campbell, 1979; Mertler & Vannatta, 2013). Figure 9 shows the research design matrix. Each variable was assigned a different color in the SPSS tool as the data was plotted on the SPSS-generated graphs. Username/password, BIO-PIN™, and BIO+PIN were evaluated for the effects the elements of Figure 9 have on them.

	Authentication	Memory	Time	Age	Gender	Account	No. Accounts	User Experience
Username/Pasword								
BIO-PIN								
BIO+PIN								

Figure 9. Research Design

The data was modeled using the MANOVA approach by applying Pillai's Trace. Pillai's Trace Test is the preferred method since it is less vulnerable to violations of the assumption of equal variance (heteroscedasticity). When significant differences were found, univariate Analysis of Variances (ANOVA) were conducted using a Welch–Satterthwaite approach. The Welch–Satterthwaite equation is used to adjust the ANOVA models for heteroscedasticity. If statistical significance was found using the univariate ANOVA, the Games-Howell test (used with unequal variance) was employed for all pair-wise comparisons.

The study used a quota sampling strategy (47 participants) that ensured to some degree that all the demographic population was represented. MANOVA sampling recommends a sample size of 100 participants. Ninety-seven individual candidates were solicited to participate, along with three clubs and organizations with varying numbers of members. Forty-seven individuals agreed to participate in the study. The problem with this strategy is that the degree of generalizability may be somewhat limited (Salkind, 2009). Table 8 provided a list of the independent, dependent, and control variables and their description that will be used in the analysis of this dissertation study.

Table 8. Variable Abbreviations and Description

Abbreviations	Descriptions
Independent Variable (IV) 1	Authentication method (multi-factor biometric authentication of a fingerprint biometrics system (BIO-PIN™) versus industry standard complex username/password versus BIO+PIN.
IV2	Time
Dependent Variable (DV) 1	Effectiveness of authentication (False Rejection)
DV2	Users' ability to remember the BIO-PIN™ versus industry standard complex username/password versus BIO+PIN
Control Variable (CV) 1	Age
CV2	Gender
CV3	User experience with computers
CV4	Number of accounts

RQ1, “What is the role of *time* on the effectiveness of authentication as measured by FRR on the BIO-PIN™ authentication method?” The authentication method (IV1) was addressed in this study by recording the number of times the user attempted to authenticate to the system using the BIO-PIN™. When using the username/password, the user results were either access granted or access denied—a simple yes or no response. In this instance, the BIO+PIN FRR was marginal because authentication was weighted more on the numerical sequences. Moreover, the effectiveness of authentication (DV1) were measured based on the actual number of successful login attempts without FRR. Then, the data collected was analyzed using SPSS.

RQ2, “What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & username/password) on the user’s ability to remember the BIO-PIN™ sequence versus BIO+PIN versus username/password?” Time (IV2) was addressed in this study over the 10-week period. Time (IV2) was based on the 10-week period of this study during 2-week, 5-week and 10-week intervals and was evaluated on its role on the effectiveness of authentication (DV2) using Mean and Standard Deviation in SPSS.

RQ3, “What is the role of *time* on the user’s *ability to remember* the BIO-PIN™ sequence versus BIO+PIN versus username/password?” The ability to remember the BIO-PIN versus username/password versus numerical BIO+PIN sequence (DV2) was used to determine how well the users remembered their BIO-PIN™, username/password, or BIO+PIN overall over the period of the study. Then, ANOVA was used on the data collected during the study to assess the overall role of authentication method (BIO-PIN™ versus username/password versus BIO+PIN) (IV1) on the ability to remember the BIO-PIN™ versus username/password versus BIO+PIN (DV2) using SPSS.

RQ4, “What is the role of *time* on the user’s *ability to remember* an industry standard complex username/password versus the BIO-PIN™ versus numerical PIN sequence (BIO+PIN)?” The *ability to remember* the BIO-PIN™ versus username/password versus BIO+PIN (DV2) was compared over time (IV2) (10-week period at 2-week, 5-week and 10-week intervals). The statistical data recorded for RQ4 was the number of times the user attempted to enter their BIO-PIN™, username/password and numerical PIN sequence BIO+PIN; and how well the users were able to remember their BIO-PIN™, username/password, or BIO+PIN during the 10-week period. The results were recorded in the spreadsheet and transferred to the SPSS tool for analysis using the MANOVA statistical analysis.

RQ4, “What is the role of the *authentication method* (BIO-PIN™, username/password, and BIO+PIN) and *time* on the *effectiveness of authentication* and the user’s *ability to remember* the BIO-PIN™ versus username/password versus the numerical PIN sequence BIO+PIN, when controlled for age (RQ4a), gender (RQ4b), volume of user accounts (RQ4c), or frequency of IT usage (RQ4d)”. RQ4 was addressed in this study using MANCOVA statistical analysis and the data from RQ1 through RQ4.This data was recorded in the SPSS tool for analysis. The results of each of these research questions (RQ4a to RQ4d) was assessed individually then compared against all the data collected and recorded. According to Fogel and Nehmad (2009), age and gender are variants that may affect the user’s ability to remember the BIO-PIN™, username/password, and the BIO+PIN.

The specific hypotheses (H3a – H3c & H4a – H4d) that relates to RQ3 and RQ4 respectively, (noted in the null format) was addressed in this study by analyzing the statistical data collected and recorded during the study to assess if there were any significant differences in remembering the BIO-PIN™, username/password, and BIO+PIN the effects of time on remembering the BIO-PIN™, username/password, and/or BIO+PIN; and individual demographics indicators such as age, gender, frequency of IT usage, and number of accounts.

Summary

Chapter 3 discussed the research methodology and the approach this research study used. The study used a quasi-experimental multiple baseline design method to evaluate the effectiveness of the BIO-PIN™ in the research questions. The participant fingerprints were collected and stored in the BIO-PIN™ application database. The users were enrolled and the BIO-PIN™ sequence was established and tested against the stored fingerprints and sequence to ensure a valid account was created and the user was authenticated.

The quota sampling size this study used was 47 participants of varying ages, gender, frequency of IT usage, and number of computer accounts. Two methods were used to validate the user. True score (yes or no) was used to grant access to the user based on the input of the correct username/password and/or BIO+PIN (fingerprints + numerical PIN). For the BIO-PIN™ sequence, an algorithm was used in which the sequence entered must meet a minimum pre-determined threshold score (>70%).

The statistical methods used for this study were Mean, Standard Deviation, ANOVA, MANOVA, and MANCOVA. MANOVA statistical analysis compared the role of the authentication method (BIO-PIN™, BIO+PIN, and username/password) on the effectiveness of authentication, and the role of time on the user's ability to remember PIN versus username/password. Additionally, MANCOVA was used to test any differences when controlled by age, gender, user experience, and number of accounts. This research study was conducted over a 10-week period with participant engagement occurring at registration week and at, 2-, 3-, and 5-week intervals. The user data was collected from the audit logs of the computer operating system and recorded in the sample BIO-PIN™ Participant Information Log. Each participant was assigned a case number that consisted of a username associated with each type of account.

Chapter 4

Results

This chapter contains the detailed results of the data analysis for this dissertation. It is organized similarly and describes the data collection process and the statistical methods used to analyze the data as outlined in Chapter 3. First, the demographic makeup of this study's participants followed by the pre-analysis data screening, data analysis methods, and results. The hypotheses results are presented as *Rejected* or *Failed to Reject the Null Hypothesis*. This chapter concludes with the findings and a summary of the results.

The BIO-PIN™ quasi-experimental consisted of 47 participants - 27 females and 20 males who actively participated in the 10-week study. A series bar graphs and tables summarizes the percentages of the demographic indicators collected for the study participants. The percent of Participants by Gender is illustrated in Figure 10.

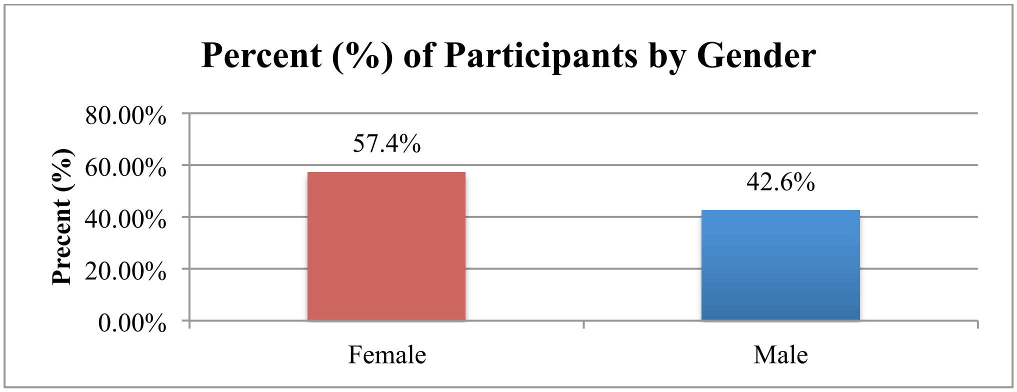


Figure 10. Summary of Participants by Gender

The number of members by age group is shown in Table 9. Figure 10 shows the bar graph of the age groups, with largest percentage of members at 27.7%. The demographic data by number of accounts is shown in Table 10 and Figure 12.

Table 9. Summary of Participants by Age, Percent, and Group Numbers

Age Group	Percent	No. of Members
18-30	12.8%	6
31-35	23.4%	11
36-50	27.7%	13
51-55	23.4%	11
56+	12.8%	6

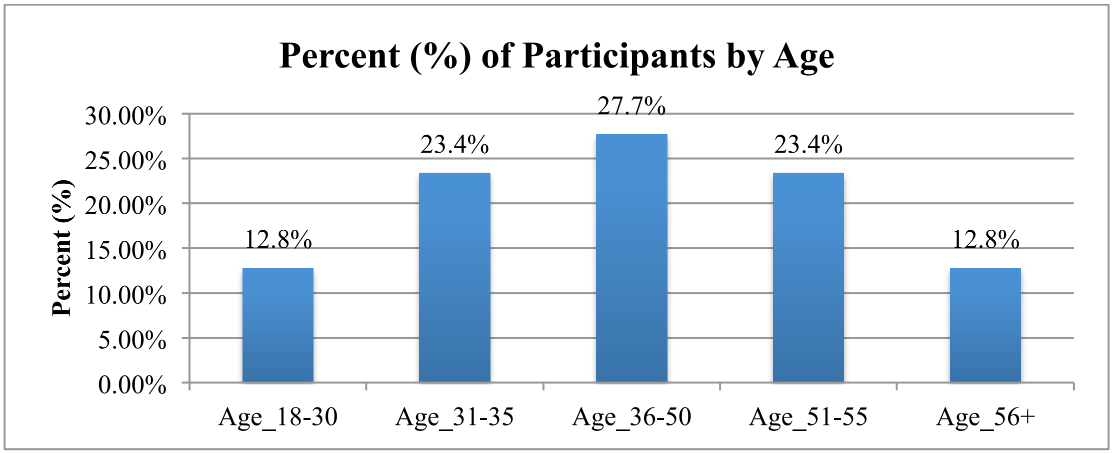


Figure 11. Summary of Participants by Age

Table 10. Summary of Participants by Number of Accounts

No. of Accounts	Percentage
1-5	8.5%
6-10	12.8%
11-15	42.6%
16+	12.8%

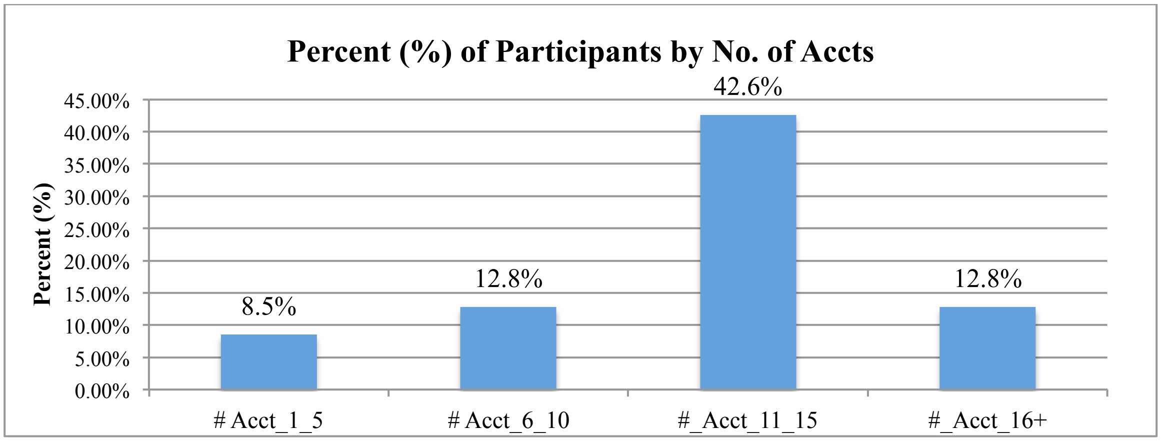


Figure 12. Summary of Participants by Number of Accounts

Table 11 and Figure 13 shows the percent of participants by their frequency of computer use in hours on a daily basis.

Table 11. Summary of Participants and Computer Usage

% of Use	Freq. of Use
19.1%	> 4 Hrs.
80.9%	5-8 Hrs.

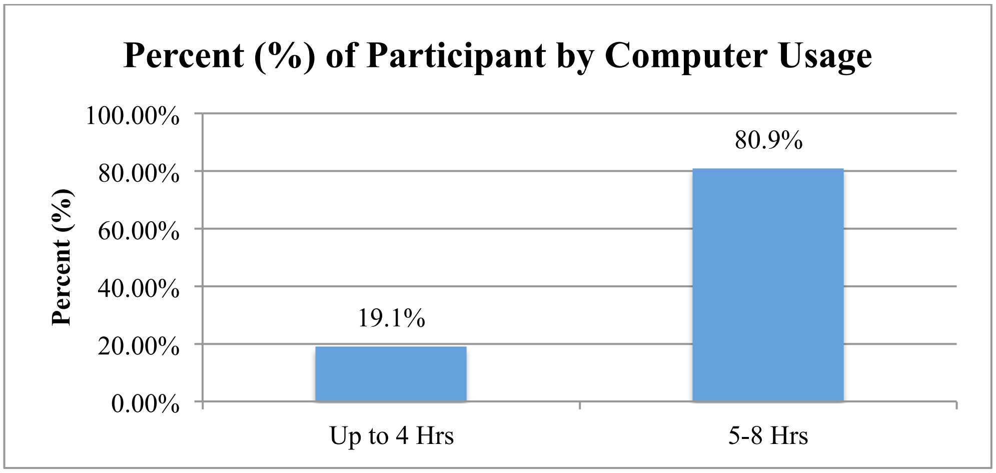


Figure 13. Percentage of Participants by Computer Usage

Pre-analysis Data Screening

Pre-analysis data screening involves a process of detecting and dealing with irregularities or problems with data collection (Levy, 2006). Pre-analysis data screening was performed to ensure consistency, accuracy, and validity of the results (Mertler & Vanatta, 2010). According to Mertler and Vanatta (2010), for the four primary reasons to conduct pre-analysis data screening, it was found that the data collected was:

1) Accurate

2) Addressed the issue of response-set.

3) Had no issue of missing data.

4) Had no extreme cases, or outliers.

This study has taken the necessary steps to address data accuracy by documenting the user's response during the quasi-experiment and recording the results immediately after the actions had been completed. The data was handled, processed, and transferred following the established procedures authorized by IRB and carried out with due diligence. All login attempts by the users were captured in the BIO-PIN™ spreadsheet and validated against the application audit logs. The data generated by this study was the reviewed to ensure any errors were caught prior to final data entry and analysis. The BIO-PIN™ application audit logs were reviewed and analyzed to validate the user authentication attempts and the allowed the measure of successes or failures for each user based on the ability to remember the authenticators or due to false rejection.

To satisfy the pre-analysis data collection and screening process user authentication attempts were closely supervised from start to finish. At the completion of the login sessions the documented results were immediately and carefully entered into the excel spreadsheet. The BIO-PIN™ application audit logs captured on each user and the results were reviewed against the excel spreadsheet. The application log is the electronic record that shows the true number of successful or unsuccessful login attempts. After review of the excel spreadsheets and the application logs, there didn't appears to be any missing data or outliers in the data collected. Based on the criteria of Mertler and Vanatta (2010), no other pre-analysis data screening was warranted.

Data Analysis

Analysis Methods

The methods used to analyze the data are discussed in this section. Descriptive statistics were calculated for all study variables and organized by each authentication method. This includes means and standard deviations for continuous measures, frequency, and accounts for categorical data. The analyses of the relationship between the variables as well as the covariates were then reported.

BIO-PIN^{TM}

Descriptive statistics for the BIO-PIN™ sequence is discussed here. Table 12 provides the descriptive statistics of the demographic indicators collected for participants in this study based on gender. The means for gender show that male users (M=1.98, SD=0.98) were more successful remembering the BIO-PIN™ sequence than females (M=2.21, SD=1.13). In all cases throughout this study the lower the mean on the ability to remember the credentials, the fewer the number of failed attempts were recorded.

Table 12. Descriptive Statistics for Gender and BIO-PIN (Mean & Standard Deviation)

Gender	Mean	SD
Female	2.21	1.13
Male	1.98	0.98

Table 13 provides the descriptive statistics of the demographic indicators collected for participants based on age for the ability to remember the credentials. The means for age distribution shows that those participants who were in the age group of 18-30 were more successful (M=1.71, SD=0.90) remembering their BIO-PIN™ sequence than all other age groups, while participants in age group 51-55 was least successful (M=2.55, SD=1.04).

Table 13. Descriptive Statistics for Age and Ability to Remember BIO-PIN (Mean & Standard Deviation)

Age Groups	Mean	SD
18-30	1.71	0.90
31-35	1.82	0.95
36-50	2.23	1.09
51-55	2.55	1.04
56+	2.00	1.00

Table 14 provides the descriptive statistics of the demographic indicators collected for study participants based on frequency of computer use. The means for frequency of use shows that participants who used computers 5-8 hours per day were more successful (M=2.09, SD=1.08) remembering the BIO-PIN™ sequence than those who used computers less than 5 hours per day (M=2.22, SD=1.05).

Table 14. Descriptive Statistics for Computer Usage and Ability to Remember BIO-PIN (Mean & Standard Deviation)

Freq. of Use	Mean	SD
Up to 4	2.22	1.05
5-8 Hrs.	2.09	1.08

Table 15 provides the descriptive statistics of the demographic indicators collected for study participants based on the number of computer accounts and the ability to remember the BIO-PIN™. The means for number of accounts shows that users with 11-15 accounts (M=1.63, SD=0.88) were most successful remembering the BIO-PIN™ sequence, while participants with 1-5 accounts (M=2.63, SD=0.80) were least successful.

Table 15. Descriptive Statistics for the Number of Accounts and Ability to Remember BIO-PIN™ (Mean & Standard Deviation)

Number of Accounts	**Mean**	**SD**
1-5	2.63	0.80
6-10	2.25	1.24
11-15	1.63	0.88
16+	2.04	0.96

Table 16 provides the descriptive statistics of the demographic indicators collected for study participants based on the mean number of false rejections. The means for the FRR of BIO-PIN™ shows that users had fewer incidents of FRR during Week 5 (M=1.28, SD=0.71) than any other time during the 10-week study. In all cases throughout this study the lower the mean on the authentication effectiveness (as measured by the FRR), the less false rejections were recorded, which indicates a higher effectiveness of the authentication method.

Table 16. Descriptive Statistics for False Rejection Rate (FRR) of BIO-PIN™ Over Time (Mean& Standard Deviation)

	Week 2		**Week 5**		**Week 10**	
	Mean	**SD**	**Mean**	**SD**	**Mean**	**SD**
BIO-PIN™	0.38	0.77	0.52	0.93	0.62	0.85

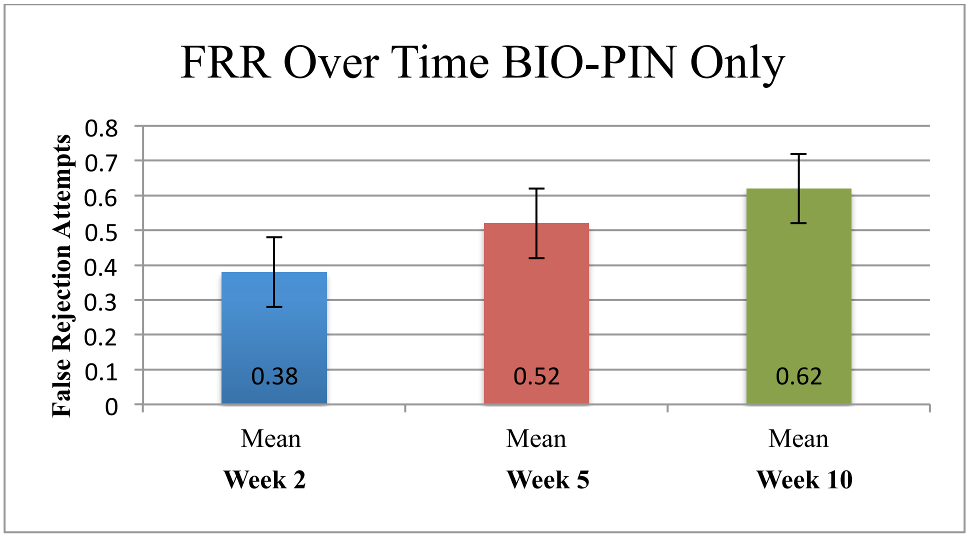


Figure 14. False Rejection by BIO-PIN™ Method

BIO+PIN

Descriptive statistics for the BIO+PIN are discussed here. Table 17 provides the Descriptive Statistics of the demographic indicators collected for study participants based on gender for BIO+PIN. The means for gender shows that male participants were more successful (M=1.65, SD=0.89) remembering the BIO+PIN sequence compared to female participants (M=1.78, SD=0.94).

Table 17. Descriptive Statistics for Gender and Ability to Remember BIO+PIN (Mean & Standard Deviation)

Gender	Mean	SD
Females	1.78	0.94
Males	1.65	0.89

Table 18 provides the descriptive statistics of the demographic indicators collected for study participants based on age. The means for age show that users who were in age group 18-30 were more successful (M=1.29, SD=0.32) remembering their BIO+PIN sequence than the rest of the groups. Members in age group 56+ were least successful (M=1.96, SD=1.00).

Table 18. Descriptive Statistics for Age and Ability to Remember BIO+PIN (Mean & Standard Deviation)

Age Groups	Mean	SD
18-30	1.29	0.32
31-35	1.39	0.78
36-50	1.93	0.92
51-55	1.93	0.96
56+	1.96	1.00

Table 19 provides the descriptive statistics of the demographic indicators collected for study participants based on frequency of computer use. The means for frequency of computer use show that users with 5-8 hours of computer use per day were more successful (M=1.65, SD=0.89) remembering their BIO+PIN sequence, than those with less than 5 hours of computer use per day (M=2.03, SD=0.97).

Table 19. Descriptive Statistics for Usage and Ability to Remember BIO+PIN (Mean & Standard Deviation)

Freq. of Use	Mean	SD
Up to 4	2.03	0.97
5-8 Hrs.	1.65	0.89

Table 20 provides the descriptive statistics of the demographic indicators collected for study participants based on the number of computer accounts. The means for number of computer accounts show that users with 11-15 accounts (M=1.38, SD=0.56) were most successful remembering their BIO+PIN sequence than the other groups. Participants with 1-5 accounts were the least successful (M=2.44, SD=0.85).

Table 20. Descriptive Statistics for Number of Accounts and Ability to Remember BIO+PIN (Mean & Standard Deviation)

Number of Accounts	Mean	SD
1-5	2.44	0.85
6-10	1.85	0.98
11-15	1.38	0.56
16+	1.58	0.86

Username/Password

Descriptive Statistics for Username and Password (UN/PW) are discussed here. Table 21 provides the Descriptive Statistics of the demographic indicators collected for study participants based on gender for the UN/PW authentication method. The means for gender shows that male users were more successful remembering the UN/PW (M=1.25, SD=0.50) than females (M=1.51, SD=0.74).

Table 21. Descriptive Statistics for Gender and Ability to Remember UN/PE (Mean & Standard Deviation)

Gender	Mean	SD
Females	1.51	0.74
Males	1.25	0.50

Table 22 provides the Descriptive Statistics of the demographic indicators collected for study participants based on age. The means for age shows users who were in age group 31-35 (M=1.20, SD=0.33) were most successful remembering their UN/PW authentication method than the other age groups. The age group 56+ was the least successful remembering their UN/PW (M=1.67, SD=0.86).

Table 22. Descriptive Statistics for Age and Ability to Remember UN/PW (Mean & Standard Deviation)

Age Groups	Mean	SD
18-30	1.29	0.38
31-35	1.20	0.33
36-50	1.27	0.44
51-55	1.66	0.93
56+	1.67	0.86

Table 23 provides the descriptive statistics of the demographic indicators collected for study participants based on frequency of computer use. The means for frequency of computer use shows that participants with 5-8 hours of computer use per day were more successful (M=2.09, SD=1.08) remembering their UN/PW authentication method than those with less than 5 hours of computer use per day (M=2.22, SD=1.05).

Table 23. Description Statistics for usage and Ability to Remember UN/PW (Mean & Standard Deviation)

Freq. of Use	Mean	SD
Up to 4	2.22	1.05
5-8 Hrs.	2.09	1.08

Table 24 provides the descriptive statistics of the demographic indicators collected for study participants based on the number of computer accounts. The means for number of computer accounts shows that participants with 11 – 15 accounts (M=1.63, SD=0.88) were most successful remembering the UN/PW authentication method than other groups. Participants with 1-5 accounts were least successful remembering their UN/PW (M=2.53, SD=0.80).

Table 24. Descriptive Statistics for Number of Accounts and Ability to Remember UN/PW (Mean & Standard Deviation)

Number of Accounts	Mean	SD
1-5	2.53	0.80
6-10	2.25	1.24
11-15	1.63	0.88
16+	2.04	0.96

Table 25 provides a summary of the most successful participants by demographic category and authentication method.

Table 25. Summary of Statistical Data Success by Demographic Category and Method

Demographic Category	BIO-PIN	BIO+PIN	UN/PW
Gender	Male	Male	Male
Age	18-30	18-30	31-35
Number of Accounts	11-15	11-15	11-15
Frequency of Computer Use	5-8 Hrs.	5-8 Hrs.	5-8 Hrs.

Addressing the Research Questions

This section of the dissertation addresses the data collection and analysis and each of the research questions and hypotheses. The tables and figures in this section provide the summary results for each of the authentication methods (BIO-PIN™, BIO+PIN, & UN/PW). For the participants using these authentication methods, the mean, and standard deviation on the number of authentication attempts for each dependent variable was analyzed for Research Question 1 and 2. The attempts range from one to five attempts over the period of the BIO-PIN™ study, (weeks 0, 2, 5, & 10). Week 0 was the registration week where users validated that the authentication methods functioned as intended and all the results were static so no additional data analysis was needed.

The independent, dependent, and control variables of the research questions were addressed using the MANOVA statistical analysis to compare the BIO-PIN™ versus username/password versus the BIO+PIN authentication method for RQ3 in order to assess the relationships noted for age, gender, user experience, and number of accounts. MANCOVA was used to address RQ4 (Cook & Campbell, 1979; Mertler & Vannatta, 2013).

The study used a quota sampling strategy (47 users) that ensured to some degree that all the demographic population was represented. Ninety-seven individual candidates were solicited to participate, along with three clubs and organizations with varying numbers of members. Forty-seven (47) individuals agreed to participate in the study. The problem with this strategy is that the degree of generalizability may be somewhat limited (Salkind, 2009). The review of the research questions and how they are addressed in the study is presented next.

RQ1: "What is the role of time on the effectiveness of authentication as measured by FRR on the BIO-PIN authentication method?" To address RQ1 a comparison of the FRR and the effectiveness was made over the 10-week period at the intervals of week 2, week 5, and week 10. The results of this analysis show that the higher the FRR the lower the effectiveness of the authentication method as illustrated in Table 25 and Figure 14. Table 25 shows the effectiveness measured by the number of attempts varied by the authentication method. Figures 14 illustrate the mean effectiveness and FRR over the 10-week period. The results of RQ1 shows that as the authentication effectiveness increased the FRR decreased during the period for all participants.

Table 26. Effectiveness by Week and FRR (Mean)

Week	FRR	Effectiveness
0	0.000	5.000
2	0.681	4.319
5	0.830	4.170
10	1.234	3.766

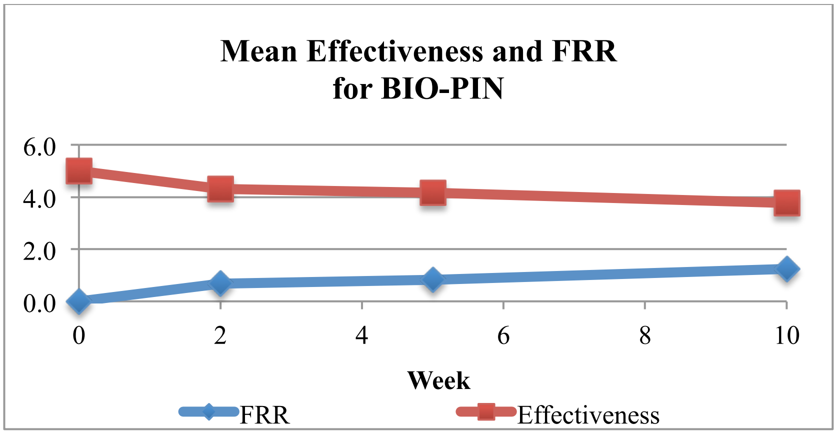


Figure 14. Mean Effectiveness for FRR and BIO-PIN

RQ2, “What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & username/password) on the users ability to remember the BIO-PIN™ sequence versus BIO+PIN versus username/password?” To address RQ2 the mean and standard deviation was made of the user’s ability to remember each authentication method over the 10-week period at the intervals of week 2, week 5, and week 10. The following formula was used:

Users’ ability to remember (1=BIO-PIN, 2=UN/PW, & 3=BIO+PIN)
Eq. 2: Memory=(5–No. of Authentication Attempts)

Table 27 shows the mean and standard deviation measured by the ability to remember the authentication methods. The results of this analysis show that the participants were more successful remembering the BIO+PIN (mean 330), followed by the BIO-PIN (mean .415), and lastly the UN/PW (mean .777). Figures 15 and 16 as well as Tables 27 and 28 illustrate the user ability to remember; the higher the number the more successful the user was at remembering the credential over the 10-week period.

Table 27. Ability to Remember Authentication Methods (Mean & Standard Deviation)

Method	BIO-PIN		UN/PW		BIO+PIN	
	Mean	**Std. Dev**	**Mean**	**Std. Dev**	**Mean**	**Std. Dev**
Memory	0.415	0.661	0.777	1.081	0.330	0.668

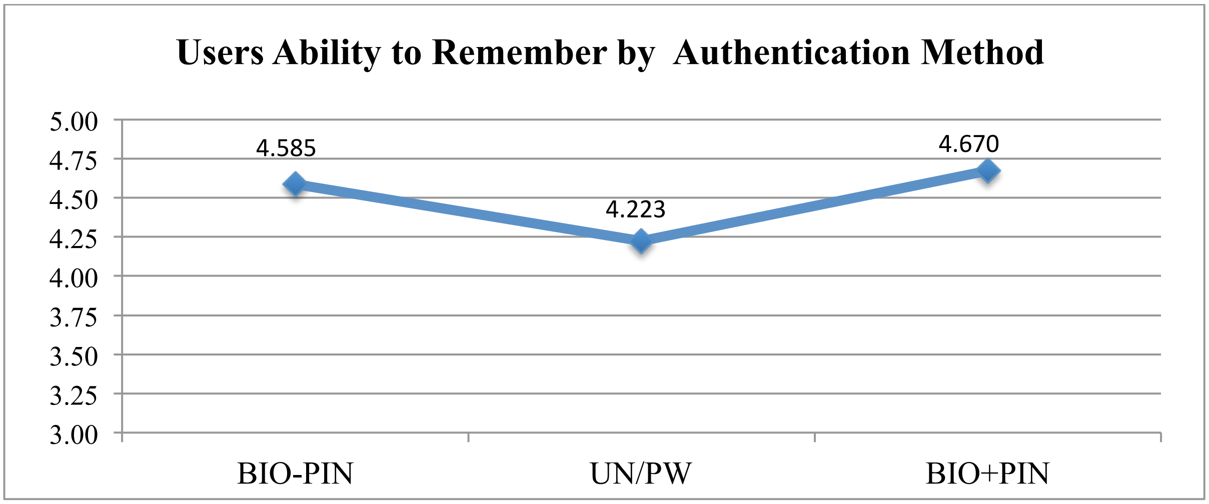


Figure 15. User Ability to Remember by Authentication Method

RQ3, "What is the role of *time* on the user's *ability to remember* the BIO-PIN$^{\text{TM}}$ sequence versus BIO+PIN versus username/password?" To address RQ3 the ANOVA method was used along with the descriptive statistics. The results of this analysis show that there is no statistically significant difference in the number of authentication attempts by method - see Table 28 and Figures 16.

Table 28. Authentication Methods by Week (Mean)

Method	WK0	WK2	WK5	WK10
BIO-PIN	5.000	4.574	4.426	4.340
UN/PW	5.000	4.085	4.043	3.766
BIO+PIN	5.000	4.681	4.596	4.404

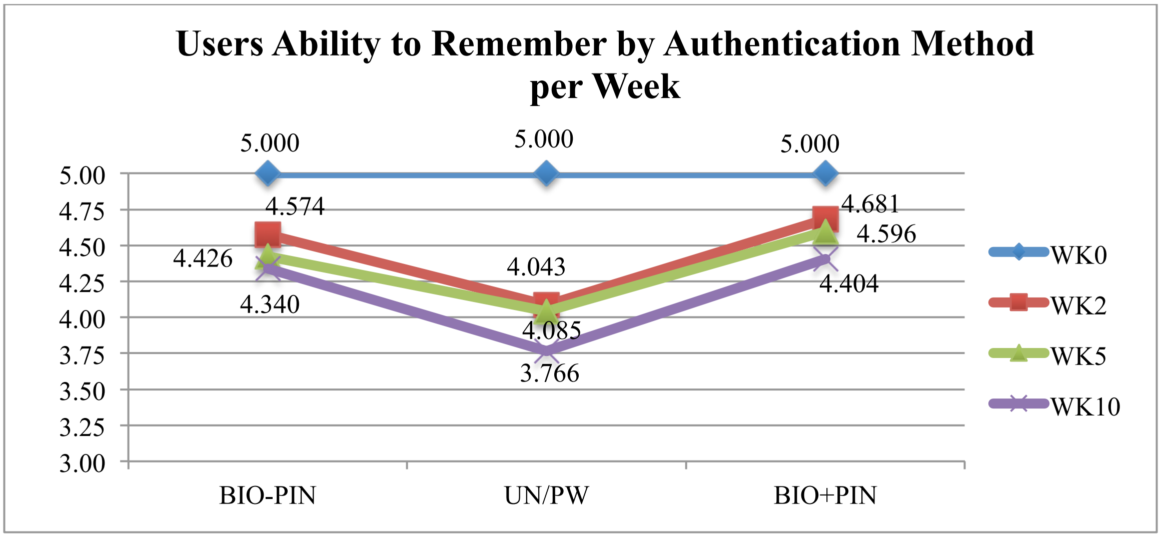


Figure 16. User Ability to Remember Authentication Method Over Time

RQ4, “What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & username/password) and *time* on the users’ *ability to remember* the BIO-PIN™ sequence versus BIO+PIN versus username/password when controlled for *age, gender, volume of user accounts, or frequency of IT usage*?” To answer RQ4 the Games-Howell comparison method was used along with the descriptive statistics. The results of this analysis show that there is a statistically significant difference in the number of authentication attempts by time. Additionally, there is no statistically significant difference on the user’s *ability to remember* the BIO-PIN™ sequence versus the BIO+PIN versus username/password by time.

> RQ4a: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & username/password) and *time* on the users’ *ability to remember* the BIO-PIN™ sequence versus BIO+PIN versus username/password when controlled for *age*? Answer Week 2: There was a statistically significant difference in the number of authentication attempts based on age, F (4,42)=3.21, p = 0.004; η^2=0.23, at week two (2).

Answer Week 5: There was a statistically significant difference in the number of authentication attempts based on age, F (4,42)=3.22, p = 0.078; η^2=0.27, at week five (5).

Answer based on time: There was a statistically significant difference in the number of authentication attempt between weeks 2 and 5, F (2,92)=23.12, p = 0.001; η^2=0.33.

RQ4b: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN & username/password) and *time* on the users' *ability to remember* PIN versus username and password when controlled for *gender*?

Answer Week 2: There was a statistically significant difference in the number of authentication attempts between the weeks 5 and 10, F (2,92)=16.57, p = 0.001; η^2=0.26.

RQ4c: What is the role of the *authentication method* (BIO-PIN™, BIO+PIN, & username/password) and *time* on the *effectiveness of authentication* and the users' *ability to remember* the BIO-PIN™ sequence versus BIO+PIN versus username/password when controlled for *volume of user accounts*?

RQ4d: What is 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 versus BIO+PIN versus username/password when controlled for *frequency of IT usage*?

Addressing the Hypotheses

The Null Hypothesis H3a through H3d, and H4a though H4d, are addressed in this section of the BIO-PIN™ Study. Three of the eight hypotheses (H3a, H3b & H3c were rejected and five failed to be reject. The hypotheses for H3 addressed if there were any significant difference in remembering BIO-PIN™, versus UN/PW, versus BIO+PIN. The detailed results of the hypothesis are addressed here:

- H3a: There will be no significant difference in remembering the sequence of the BIO-PIN™ over time (Week 0, Week 2, Week 5, & Week 10).
- Answer: There is significant difference in remembering the sequence of the BIO-PIN™ over time (F(3,187)=10.679, p<0.001
- H3b: There will be no significant difference in remembering an industry standard complex username/password over time (Week 0, Week 2, Week 5, & Week 10).
- Answer: There is significant difference in remembering the sequence of the username/password over time (F(3,187)=13.995, p<0.001
- H3c: There will be no significant difference in remembering the BIO+PIN over time (Week 0, Week 2, Week 5, & Week 10).
- Answer: There is significant difference in remembering the sequence of the BIO+PIN over time (F(3,187)=7.131, p<0.001
- H3d: There will be no significant difference in remembering the BIO-PIN™ sequence versus BIO+PIN versus username/password over time (Week 0, Week 2, Week 5, & Week 10).
- Answer: Week 0: There is NO significant difference in remembering the BIO-PIN™ sequence versus BIO+PIN versus username/password.
- In Week 2, Week 5, and Week 10: There is significant difference in remembering the BIO-PIN™ sequence versus BIO+PIN versus username/password (p<0.001)

The hypotheses for H4 addressed any significant differences in remembering BIO-PIN™, versus UN/PW, versus BIO+PIN when compared for age, gender, number of accounts, and frequency of use. The detailed results of the hypothesis are addressed here:

- H4a: There will be no significant difference in remembering an industry standard complex username/password, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for age.
- Answer: There was a statistically significant difference in the number of authentication attempts based on age, F (4,42)=3.22, **p* = 0.022; ** p = 0.004; *** p = 0.041; η^2=0.27, at week five. (Note: * = age 56+ versus 18-30; ** = age 56+ versus 31-35; *** age 56+ versus 36-50)
- H4b: There will be no significant difference in remembering an industry standard complex username/password, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for gender.
- Answer: There is a statistically significant difference in the number of authentication attempts between the weeks based on Gender, F (2,91)=3.13, *p* = 0.049; η^2=0.06. However, there was no statistically significant difference in the number of authentication attempts by any independent variable.
- H4c: There will be no significant difference in remembering an industry standard complex username/password, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for volume of user accounts.
- Answer: There was no significant difference in remembering an industry standard complex username/password, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for volume of user accounts.

- H4d: There will be no significant difference in remembering an industry standard complex username/password, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for frequency of IT usage.
- Answer: There was no significant difference in remembering an industry standard complex username/password, when compared to the BIO-PIN™ sequence, the BIO+PIN, and controlled for frequency of IT usage.

Findings

The findings of the data analysis performed on the Research Questions and Hypotheses of the BIO-PIN™ Study were presented here in Chapter 4. The BIO-PIN™ quasi-experimental study shows that there were 47 users including 27 females and 20 males who actively participated in and completed the 10-week study. The analysis shows that of the 47 users 57.4% female and 42.6% male. The largest group was between the ages of 36-50 (27.7%), and that 42.6% had between 11-15 user accounts at various sites on the Internet. The findings verified that 80.9% of the participants used computer 5-8 hours per day. Of the 47 participants in this study 25 (53%) selected a PIN that consisted of a number pattern (2288, 1111, or 5665), sequence (1234 or 9876), or calendar year (1954 or 2013).

The data collected supported the theory that there were some statistically significant differences noted in authentication attempts based on age, at week 2 and week 5. Statistically significant differences were also noted in the users ability to remember the authentication based on the number of attempts over time. The descriptive statistics tables include the demographic data for the users by age, gender, number of accounts, and frequency of computer use. The tables provided mean, and standard for the authentication attempts as well as p-value over the period of the BIO-PIN study (weeks 0, 2, 5, & 10).

RQ1 compared the FRR and the effectiveness of the BIO-PIN over the 10-week period. The results of this analysis show that the higher the FRR the lower the effectiveness of the authentication method. RQ2 showed the mean and standard deviation of the user's ability to remember each authentication method over the 10-week period. RQ3 used the ANOVA method along with the descriptive statistics. The results of this analysis showed there is no statistically significant difference in the number of authentication attempts by method. RQ4 used the Games-Howell comparison method along with the descriptive statistics. The results of this analysis show there was a statistically significant difference in the number of authentication attempts over time. Additionally, there is no statistically significant difference on the user's ability to remember the BIO-PIN™ sequence versus the BIO+PIN versus username/password over time.

Summary of Results

There were four (4) research questions and eight (8) hypotheses addressed in this study. The research questions found that there were statistically significant differences between authentication methods at week 2 and week 5 (H3a, H3b, & H4c) had statistically significant differences in the number of authentication attempts and were rejected. The hypotheses (H3d, H4a through H4d) that failed to be rejected were based on age, (at Week 2 & Week 5), between weeks, between authentication methods, and between authentication method over time. It appears that over time, users authenticating with UN/PW experienced the most failed authentication attempts, followed by BIO-PIN™, and

BIO+PIN with the least number of failed attempts even when various statistical methods were used to correct for any defects or anomalies.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

In this chapter, conclusions are drawn and discussed based upon the analysis performed within this study. The research questions are examined in context of the results achieved along with any limitations of the study. The implications for study and the contribution to the body of knowledge within the study of Information Systems, Information Security, Information Assurance, Cyber Security, and biometric is discussed as well as recommendations for future research. Finally, a summary concludes this chapter of the study.

Conclusion

To reiterate, the main goal of this study was to determine the effectiveness of authentication, and the users' ability to remember the BIO-PIN™ versus the BIO+PIN versus UN/PW over a 10-week period of time at intervals of 2-weeks, 5-weeks and 10-weeks. This study was built on previous scholarly works and research conducted by Hayashi, et al. (2008) where users authenticate by selecting a series of pictures in a sequence—'something the user knows.' With the BIO-PIN™ as something the user is (a fingerprint) and something the user knows (the correct sequence the fingertip and/or finger segment are presented or selected), the user validation may be strengthened. Several researchers of note (including Furnell, 2007; Furnell, 2013; Furnell et al., 2000; Jain et al., 2006; Mujeye & Levy 2013; Woodard & Flynn 2005) and others have conducted research in this area.

The conclusion of the BIO-PIN™ study suggests that some users in all demographic distribution had difficulties remembering their authenticators. The method most users had difficulties remembering was username and industry standard password. The analysis from the top three members groups (age groups 31-35, 36-50, & 51-55) shows that age was not a differentiating factor when it came to the number of successful logins over time base on the number of participants in the groups. The gender demographic data suggested that men were more successful than women with login attempts over the sessions conducted. The data shows that the BIO+PIN authentication method was easiest to remember with the most number of successful logins and the least number of failed attempts. The data shows that the BIO-PIN™ authentication method was the second easiest to remember. It appears that users had the most difficulty remembering their industry standard password.

Four research questions and eight hypotheses were developed for this quasi-experimental research study that were analyzed and discussed based on the data collected with the BIO-PIN™ application. RQ1 discussed the effectiveness of the BIO-PIN™ based on the FRR over the 10-week period. The results of this analysis show that the higher the FRR the lower the effectiveness of the authentication method. RQ2 discussed the user's ability to remember each authentication method over the 10-week period. It validated that users were more successful with BIO+PIN than other methods. RQ3 used the ANOVA method along with the descriptive statistics. The results of this analysis showed there is no statistically significant difference in the number of authentication attempts by method.

RQ4 used the Games-Howell comparison method along with the descriptive statistics. The results of this analysis show there was a statistically significant difference in the number of authentication attempts over time. Additionally, there is no statistically significant difference on the user's ability to remember the BIO-PIN™ sequence versus the BIO+PIN versus username/password over time.

Limitations are factors that were difficult to control. There were a few notable limitations for this study. Limitations included the possible threat to internal validity of users generating familiar passwords and PIN numbers. To minimize this threat, the users were trained in password creation and asked to create a totally new password based on a password creation technique (using a password scheme based on a phrase the user found easy to remember). However, participants still created 4-digit numerical PINs based on personal events, number patterns or sequences (DataGenetics, 2012).

Implications

The results of this study contributed notably to the body of knowledge and had several implications within the field of information systems, information security, information assurance, cyber security, as well as future research in the domain of authentication methods. The research includes a literature review in order to understand how users remember authentication methods such as the BIO-PIN™ when compared with UN/PW and BIO+PIN. The results of the study implies that these authentication methods may be more secure since previous studies have shown that users do not adequately protect their UN/PW and their numerical PINs are easily compromised because of the way they are created leaving them vulnerable to compromise. Authentication methods like the BIO-

PIN™ and BIO+PIN might be suitable alternatives that are easier to remember and less likely to be compromised. This is particularly true since the BIO-PIN™ sequence relies on a live subject with knowledge of the sequence and an aliveness test to validate the participant is a live subject and not a robot or other brute force attack tool. The BIO+PIN authentication method relies on the fingerprint biometric and a numerical PIN. The PIN is suspected of being easy to compromise because of the limitation with the number of possible sequences. However, with the addition of the fingerprint biometric the percent of possible compromise may be dramatically reduced.

The biometric fingerprint readers selected for the study provided the aliveness test and collected enough minutiae to identify most participants. It appears that some women with small hands experienced a more difficult time with false rejection perhaps due to the minimum amount of minutiae collected at the time of registration that was never quite enough minutiae presented at subsequent login sessions. This factor is an area for further investigation in any subsequent studies.

Recommendations

Additional research ideas may include conducting a vulnerability assessment or static code analysis of the BIO-PIN™ application to determine how difficult it would be hack into the application and compromise the authenticators. There could also be an update to the BIO-PIN application code to include security best practices making it less likely to exploitation. One observation noted during the study was that some participants appeared to have difficulty remembering all the authenticators required for the study, which included the BIO-PIN™ sequence, UN/PW, BIO+PIN. More research conducting a study comparing the BIO-PIN™ versus BIO+PIN without the username and password might be warranted. This was particularly noticeable during the initial registration. By eliminating one of the authentication methods user may feel more comfortable and less challenged to remember so many different authentication methods.

During the BIO-PIN™ Study it was observed that users immediately wanted to write down their usernames and passwords. This appears to be a common practice until they were comfortable remembering the new authenticator. A second research topic would be to conduct a survey on how users create and remember passwords or other authentication methods. This survey would include questions on the number of computer accounts they have and their experience using computers and information systems.

Additionally, another potential research study might be to test voice recognition software and a numerical PIN to see if users are more comfortable with this authentication method. This study would include an independent voice recognition system where the user has something he or she has, voice and something he or she knows, the name or PIN number spoken. The user would speak the PIN, "One, Two, Three, Four" and the user independent section identified that a person said "1234". The PIN 1-2-3-4, would then be used to look up an individual voiceprint of PIN user 1234 and would compare the numbers spoken to the users voice print to authenticate the access request. Being numbers, made the voice print relatively small and the use of the PIN to index the voiceprints made the look-up relatively fast (assuming use of a random PIN like the last 4 of SSN).

The concept may have an added benefit of being free, not requiring any type of external device, as most computers, tablets and phones already have a microphone. A simple intercom type device would be used at door entrances, which may already be there as well. It enforced the use of something you had (voice) with something you know (PIN). Even if you overheard the person, you would not be able to duplicate the voice. It does not require contact with skin and pathogens or will it ever get dirty enough to inhibit sound entry.

Summary

The research problem addressed was that traditional user authentication methods, such as UN/PWs, still pose a significant vulnerability when accessing information systems. Valid literature supporting the need for this research was presented as well as the main goal and specific research questions. The main goal of this research study examined the role of the authentication method (BIO-PIN$^{\text{TM}}$ versus the BIO+PIN versus UN/PW) and time on the effectiveness of authentication, as well as users' ability to remember BIO-PIN$^{\text{TM}}$ versus the BIO+PIN versus UN/PW. Prior literature that supported the main goal of this research was also presented (Furnell, 2007; Hayashi et al., 2008; Jain et al., 2006; Maty´aˇs & R´ıha 2010; Mujeye & Levy, 2013; Ross, 2007; Woodard & Flynn, 2005).

The main contributions of this study were to advance the understanding of users' authentication to information systems, security threats, problems with user authentication and personal information sharing habits, as well as information sharing practices. Information gained from the results of this study may help organizations develop better approaches to securing their users' personal and organizational information. Implementation of information security policy that addressed these types of access controls and authentication concerns may lead to a reduction of breaches and compromises.

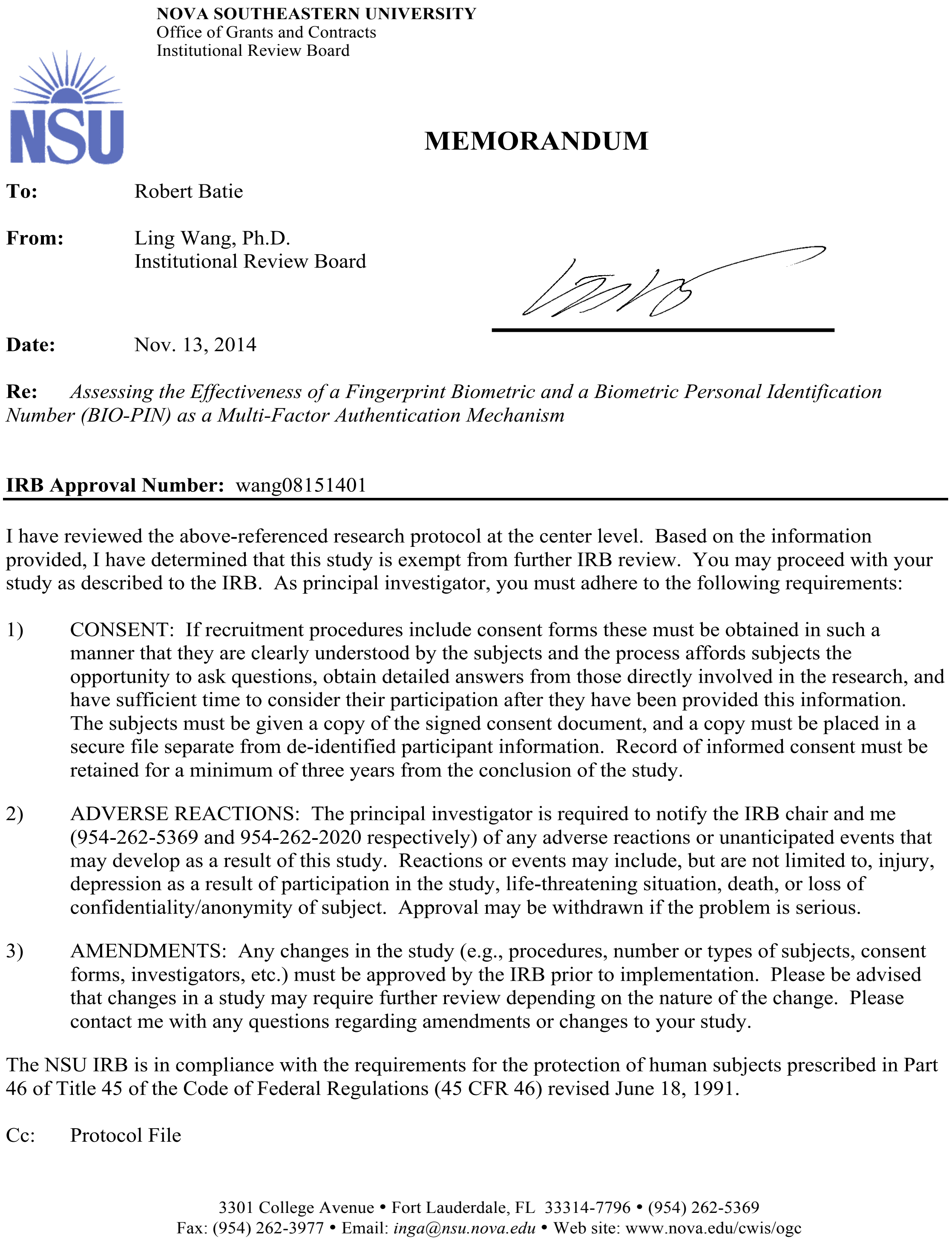
The study used a quasi-experimental multiple baseline design method to evaluate the effectiveness of the BIO-PIN™ in the research questions. The participant fingerprints were collected and stored in the BIO-PIN™ application database. The participants were enrolled. Three authentication methods were established and tested to ensure successful enrollment, a valid account was created and the user was authenticated.

The quota sampling size for the study was 47 participants of varying demographics of ages, gender, frequency of IT usage, and number of computer accounts. Two methods were used to validate the user. True score (yes or no) was used to grant access to the user based on the input of the correct username/password and/or BIO+PIN (fingerprints + numerical PIN) and algorithm with a pre-determined threshold score (>70%) for the BIO-PIN™ sequence. The statistical methods used were Mean and Standard Deviation for RQ1 and RQ2, MANOVA, and MANCOVA for multivariate analysis for RQ3 and RQ4. MANOVA statistical analysis compared the role of the authentication method (BIO-PIN™, BIO+PIN, and username/password) on the effectiveness of authentication, and the role of time on the user's ability to remember PIN versus username/password. Additionally, MANCOVA was used to test any differences when controlled by age, gender, user experience, and number of accounts. This research study was conducted over a 10-week period with participant engagement occurring at registration week and at, 2-, 3-, and 5-week intervals.

The four (4) research questions and eight (8) hypotheses addressed in this study found that there were statistically significant differences between authentication methods over time, and statistically significant differences in the number of authentication attempts. Three of the hypotheses that failed to be rejected were based on age, (at Week 2 & Week

5), between weeks, between authentication methods, and between authentication method over time. It appears that over time, users authenticating with UN/PW experienced the most failed authentication attempts, followed by BIO-PIN™, and BIO+PIN with the least number of failed attempts was more successful even when various statistical methods were used to correct for any defects or anomalies.

Appendix A



NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Robert Batie

From: Ling Wang, Ph.D.
Institutional Review Board

Date: Nov. 13, 2014

Re: *Assessing the Effectiveness of a Fingerprint Biometric and a Biometric Personal Identification Number (BIO-PIN) as a Multi-Factor Authentication Mechanism*

IRB Approval Number: wang08151401

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

APPENDIX B

Participant Solicitation Email, and Presentation Information

This Appendix provides an example of the solicitation email and the BIO-PIN$^{\text{TM}}$ presentation sent to potential to participants of the study.

From: rbatie@verizon.net
To: rbatie@verizon.net
Date: 07/27/2015 02:05 PM
Subject: The BIOPIN Study-My Research Project

All,
I am in the final stages of my dissertation getting ready to start the data collection in order to complete the quasi-experiment and write my final report. I need your help! I am looking for 50 candidates to participate in the BIO-PIN Study.

The BIO-PIN Study will examine and compare the users ability to remember the BIO-PIN Sequence vs. Industry standard username/password vs. a BIO+4 digit PIN over a 10-week period.

Please go to the https://thebiopinstudy.com and spend a few minutes looking at the website that explains my study.

If you are interested send me an email at rbatie@verizon.net and I will fill you in with the latest details on when the study begins and where it will take place. If you are unavailable, feel free to recommend someone who might be interested. Please reply either way so I will know that you had the opportunity to explore this idea.

Thank you in advance for your support
V/r

R.B. "Bob" Batie, CISSP-ISSEP, CAP
Ph.D Candidate, Nova Southeastern University
rbatie@verizon.net or rbatie@nova.edu

Reply to BIO-PIN Study Participants Email

From: rbatie@verizon.net
Date: Thursday, August 6, 2015 at 5:42 PM
To: Robeba <rbatie@verizon.net>
Subject: The BIO-PIN Study

Dear BIO-PIN Study participants.
Thanks you for taking an interest in the BIO-PIN study and sharing your time in helping me achieve this goal. Some of you are still considering joining the study and others have already committed. As promised I have attached a presentation that will help you understand what we are doing and how important your support will be in this effort. I cannot thank you enough! So, Thank you! Thank you! Thanks you!

As you review the Power Point you will notice what the Participants will be required to do and the schedule of the four sessions. There are two days for Northern Virginia, Dulles and Woodbridge and two days for Tampa/St. Pete/Largo for the four sessions. The first step is week 0 and registration. More information on locations will be emailed to specific participants.

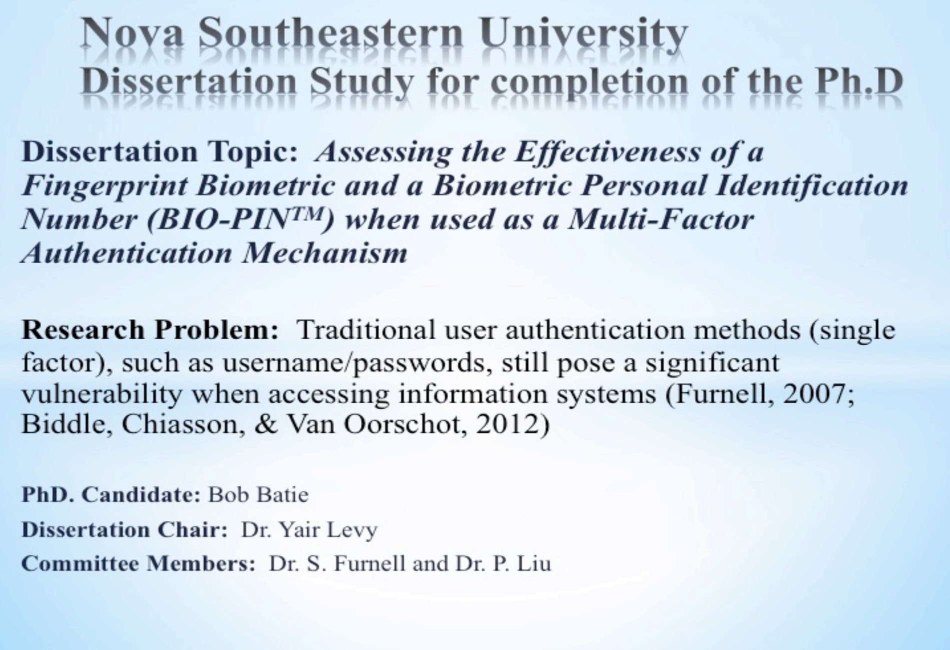
You will see that after registration the time it takes to complete the login and send an email is less than 10 minutes. I am still taking recommendations for any new participants so please send me a list of friends and relatives.

If you have any questions or concerns please feel free to send me an email.
Again, thank you for your support.
V/r

R.B. "Bob" Batie, CISSP-ISSEP, CAP
Ph.D Candidate, Nova Southeastern University
rbatie@verizon.net or rbatie@nova.edu

BIO-PIN Solicitation Presentation

The BIO-PIN Solicitation Presentation was used to educate and recruit subjects to be part of the Dissertation Study. It was sent out to those respondents who wanted additional information about the study or who agreed to participate based on the email. It was also presented at the kickoff and registration sessions for each group.

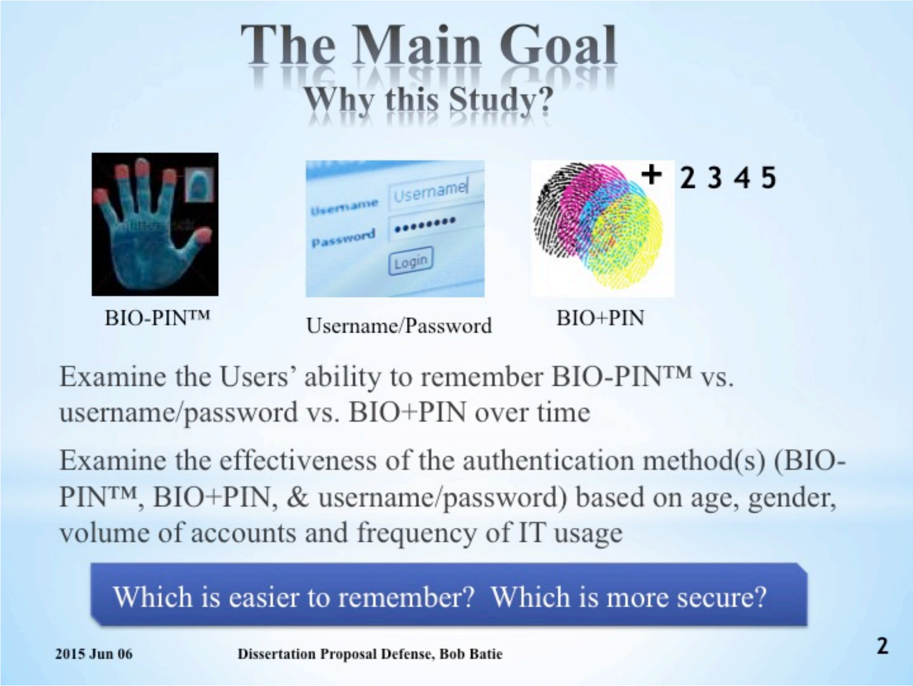


Nova Southeastern University
Dissertation Study for completion of the Ph.D

Dissertation Topic: ***Assessing the Effectiveness of a Fingerprint Biometric and a Biometric Personal Identification Number (BIO-PIN^{TM}) when used as a Multi-Factor Authentication Mechanism***

Research Problem: Traditional user authentication methods (single factor), such as username/passwords, still pose a significant vulnerability when accessing information systems (Furnell, 2007; Biddle, Chiasson, & Van Oorschot, 2012)

PhD. Candidate: Bob Batie
Dissertation Chair: Dr. Yair Levy
Committee Members: Dr. S. Furnell and Dr. P. Liu


+ 2 3 4 5
Username
Password
Username
Login

The Main Goal

Why this Study?

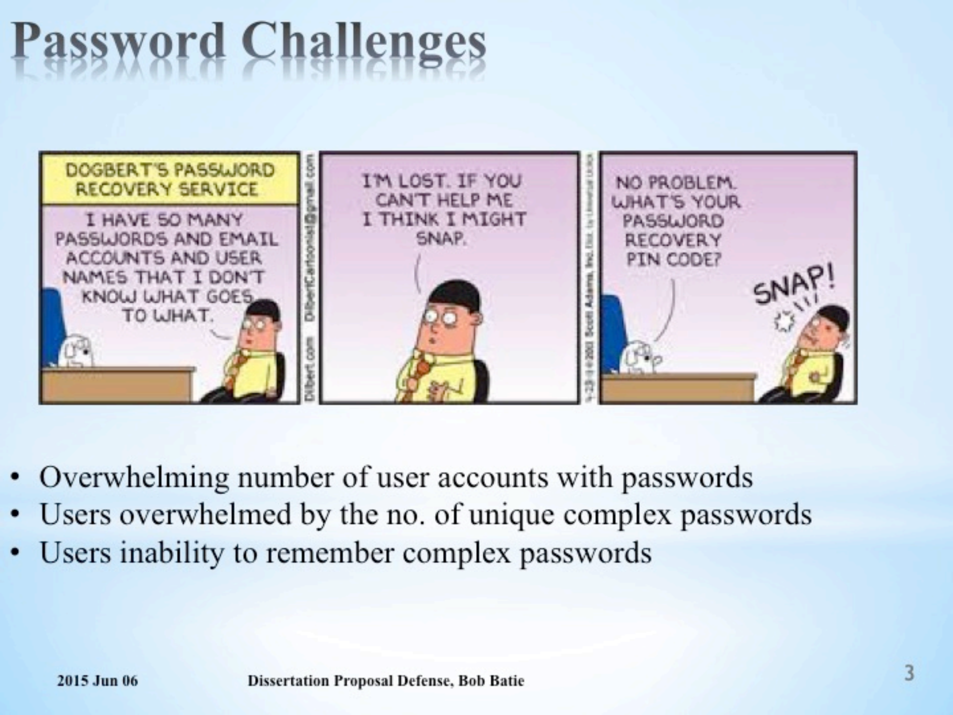
BIO-PIN™ Username/Password BIO+PIN

Examine the Users' ability to remember BIO-PIN™ vs. username/password vs. BIO+PIN over time

Examine the effectiveness of the authentication method(s) (BIO-PIN™, BIO+PIN, & username/password) based on age, gender, volume of accounts and frequency of IT usage

Which is easier to remember? Which is more secure?

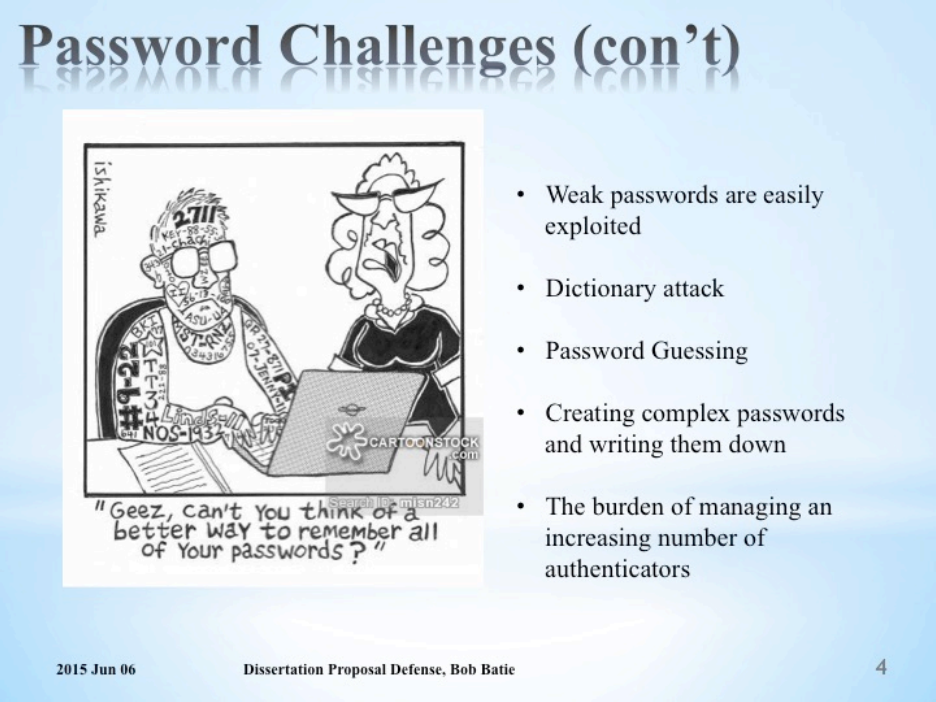
2015 Jun 06 Dissertation Proposal Defense, Bob Batie 2


DOGBERT'S PASSWORD RECOVERY SERVICE
I HAVE SO MANY PASSWORDS AND EMAIL ACCOUNTS AND USER NAMES THAT I DON'T KNOW WHAT GOES TO WHAT.
I'M LOST. IF YOU CAN'T HELP ME I THINK I MIGHT SNAP.
NO PROBLEM. WHAT'S YOUR PASSWORD RECOVERY PIN CODE?
SNAP!

Password Challenges

- Overwhelming number of user accounts with passwords
- Users overwhelmed by the no. of unique complex passwords
- Users inability to remember complex passwords

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 3

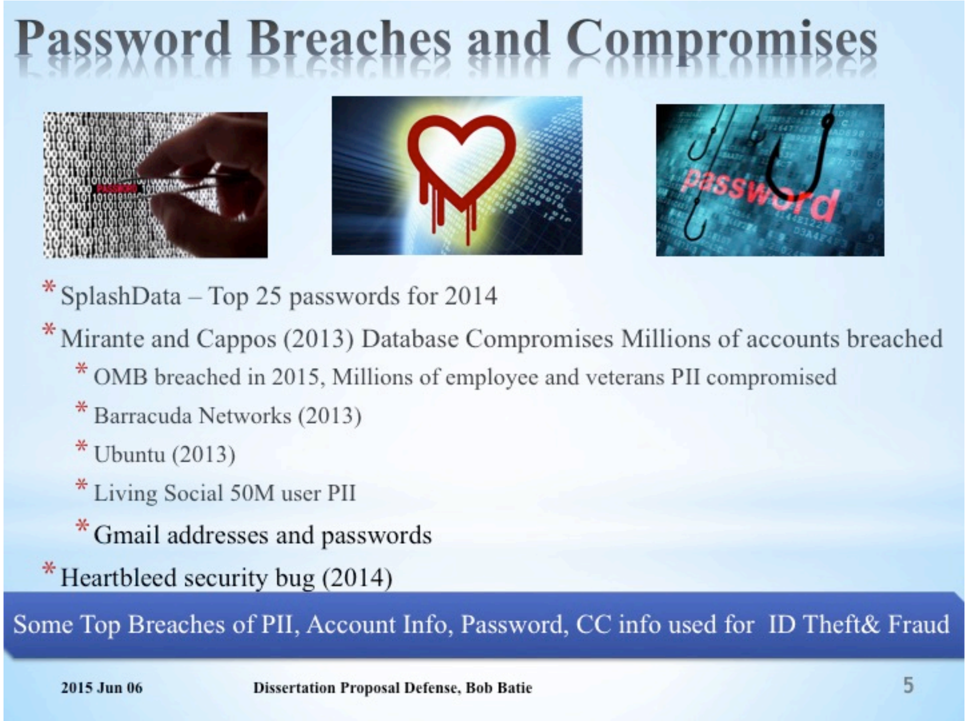


Password Challenges (con't)

ishikawa
"Geez, can't you think of a better way to remember all of your passwords?"
CARTOONSTOCK .com
Search ID: misn242

- Weak passwords are easily exploited
- Dictionary attack
- Password Guessing
- Creating complex passwords and writing them down
- The burden of managing an increasing number of authenticators

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 4

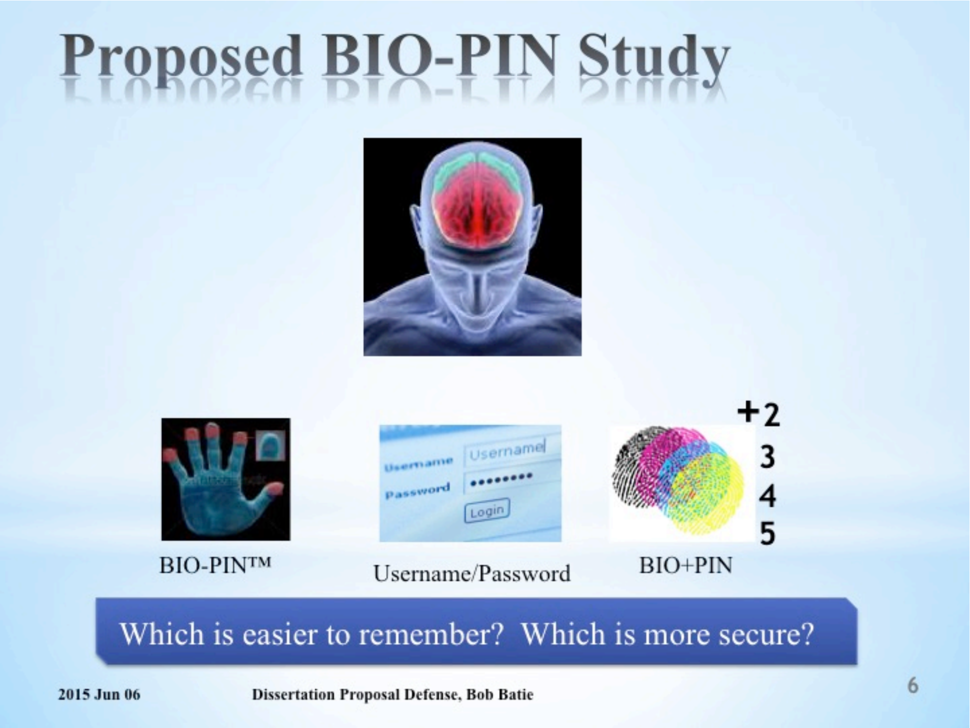


Password Breaches and Compromises

- SplashData – Top 25 passwords for 2014
- Mirante and Cappos (2013) Database Compromises Millions of accounts breached
  - OMB breached in 2015, Millions of employee and veterans PII compromised
  - Barracuda Networks (2013)
  - Ubuntu (2013)
  - Living Social 50M user PII
  - Gmail addresses and passwords
- Heartbleed security bug (2014)

Some Top Breaches of PII, Account Info, Password, CC info used for ID Theft& Fraud

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 5


Username
Password
Username
••••••••
Login

Proposed BIO-PIN Study

+2
3
4
5

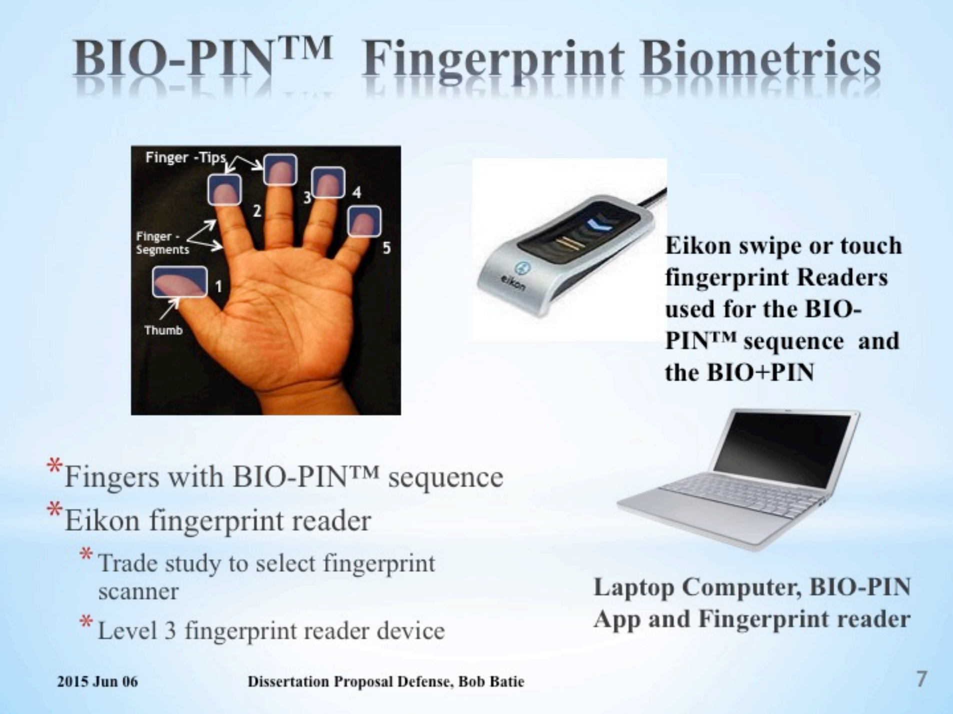
BIO-PIN™

Username/Password

BIO+PIN

Which is easier to remember? Which is more secure?

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 6


Finger -Tips
Finger - Segments
Thumb
1
2
3
4
5
eikon

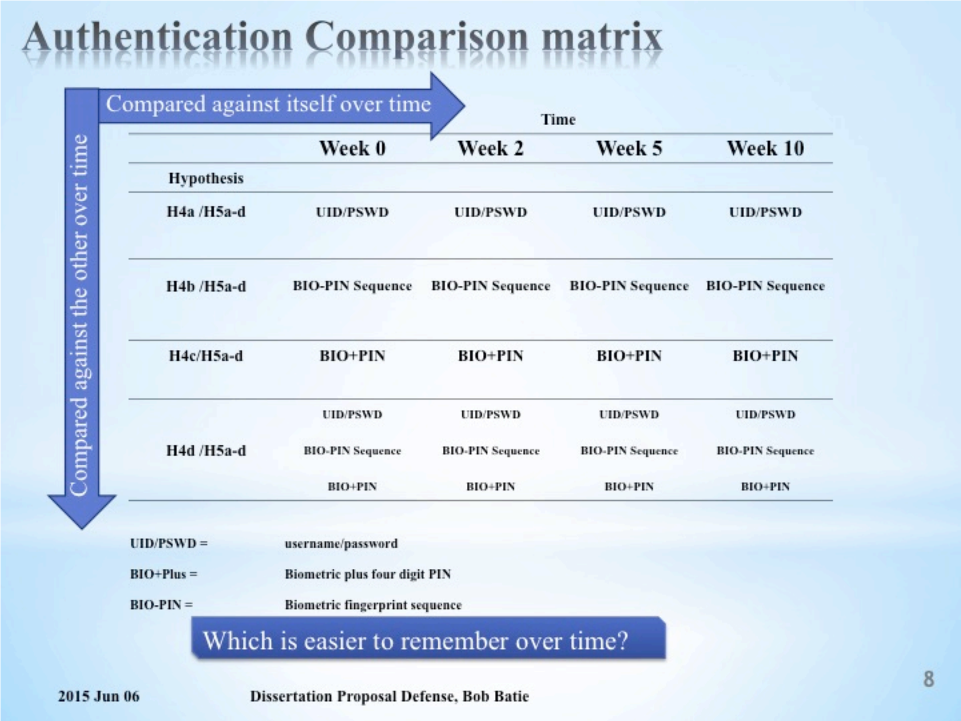
BIO-PIN™ Fingerprint Biometrics

Eikon swipe or touch fingerprint Readers used for the BIO-PIN™ sequence and the BIO+PIN

- *Fingers with BIO-PIN™ sequence
- *Eikon fingerprint reader
  - *Trade study to select fingerprint scanner
  - *Level 3 fingerprint reader device

Laptop Computer, BIO-PIN App and Fingerprint reader

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 7



Authentication Comparison matrix

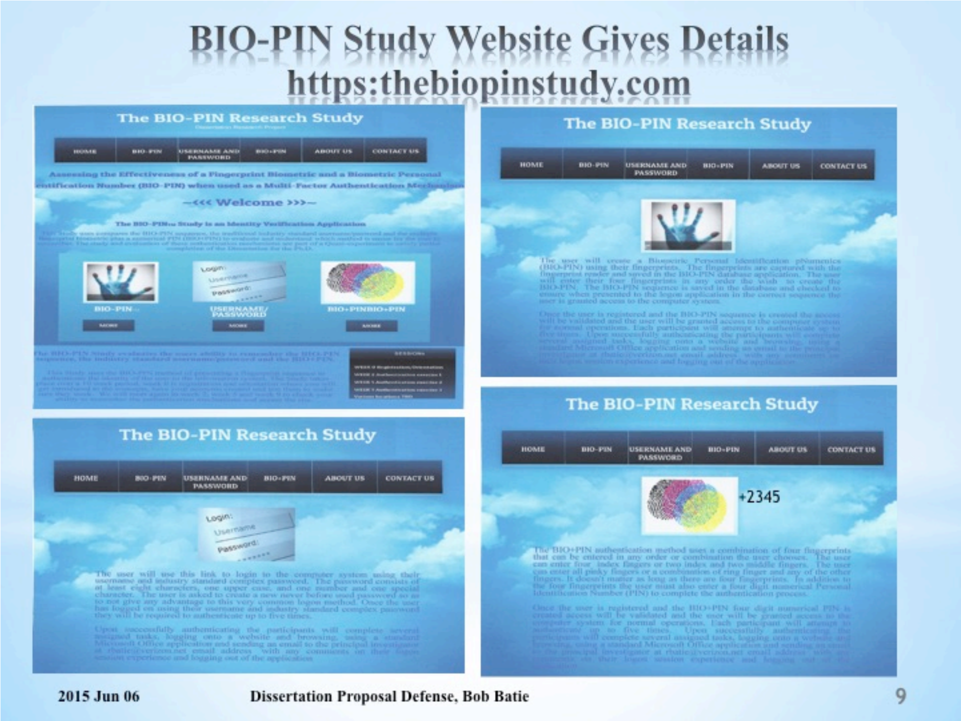
Compared against itself over time
Compared against the other over time

	Time			
	Week 0	Week 2	Week 5	Week 10
Hypothesis				
H4a /H5a-d	UID/PSWD	UID/PSWD	UID/PSWD	UID/PSWD
H4b /H5a-d	BIO-PIN Sequence	BIO-PIN Sequence	BIO-PIN Sequence	BIO-PIN Sequence
H4c/H5a-d	BIO+PIN	BIO+PIN	BIO+PIN	BIO+PIN
H4d /H5a-d	UID/PSWD BIO-PIN Sequence BIO+PIN	UID/PSWD BIO-PIN Sequence BIO+PIN	UID/PSWD BIO-PIN Sequence BIO+PIN	UID/PSWD BIO-PIN Sequence BIO+PIN

UID/PSWD =	username/password
BIO+Plus =	Biometric plus four digit PIN
BIO-PIN =	Biometric fingerprint sequence

Which is easier to remember over time?

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 8



BIO-PIN Study Website Gives Details https:thebiopinstudy.com

The BIO-PIN Research Study

Dissertation Research Project

Assessing the Effectiveness of a Fingerprint Biometric and a Biometric Personal Identification Number (BIO-PIN) when used as a Multi-Factor Authentication Mechanism

—<<< Welcome >>>—

The BIO-PIN™ Study is an Identity Verification Application

This Study uses compares the BIO-PIN sequence, the traditional industry standard username/password and the multiple fingerprint biometric plus a numerical PIN (BIO+PIN) to evaluate and understand which method is easier for the user to remember. The study and evaluation of these authentication mechanisms are part of a Quasi-experiment to satisfy partial completion of the Dissertation for the Ph.D.

The BIO-PIN Study evaluates the users ability to remember the BIO-PIN sequence, the industry standard username/password and the BIO+PIN.

This Study uses the BIO-PIN method of presenting a fingerprint sequence to authenticate the identity of the user to the information system. The Study takes place over a 10 week period, week 0 is registration and orientation where you will get introduced to the [illegible], have your accounts created and test them to make sure they work. We will meet again in week 2, week 5 and week 9 to check your ability to remember the authentication mechanisms and access the site.

SESSIONS

WEEK 0 Registration/Orientation
WEEK 2 Authentication exercise 1
WEEK 5 Authentication exercise 2
WEEK 9 Authentication exercise 3
Various locations TBD

The BIO-PIN Research Study

The user will create a Biometric Personal Identification pNumerics (BIO-PIN) using their fingerprints. The fingerprints are captured with the fingerprint reader and saved in the BIO-PIN database application. The user will enter their four fingerprints in any order the wish to create the BIO-PIN. The BIO-PIN sequence is saved in the database and checked to ensure when presented to the logon application in the correct sequence the user is granted access to the computer system.

Once the user is registered and the BIO-PIN sequence is created the access will be validated and the user will be granted access to the computer system for normal operations. Each participant will attempt to authenticate up to five times. Upon successfully authenticating the participants will complete several assigned tasks, logging onto a website and browsing, using a standard Microsoft Office application and sending an email to the principal investigator at rbatie@verizon.net email address with any comments on their logon session experience and logging out of the application.

The BIO-PIN Research Study

The user will use this link to login to the computer system using their username and industry standard complex password. The password consists of at least eight characters, one upper case, and one number and one special character. The user is asked to create a new never before used password so as to not give any advantage to this very common logon method. Once the user has logged on using their username and industry standard complex password they will be required to authenticate up to five times.

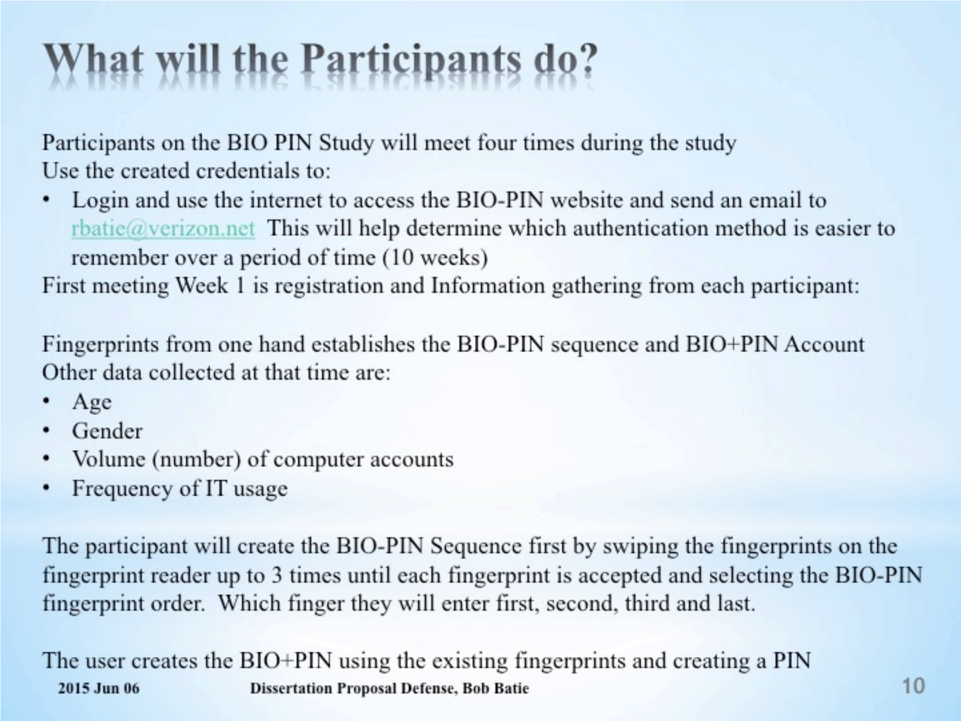
Upon successfully authenticating the participants will complete several assigned tasks, logging onto a website and browsing, using a standard Microsoft Office application and sending an email to the principal investigator at rbatie@verizon.net email address with any comments on their logon session experience and logging out of the application.

The BIO-PIN Research Study

The BIO+PIN authentication method uses a combination of four fingerprints that can be entered in any order or combination the user chooses. The user can enter four index fingers or two index and two middle fingers. The user can enter all pinky fingers or a combination of ring finger and any of the other fingers. It doesn't matter as long as there are four fingerprints. In addition to the four fingerprints the user must also enter a four digit numerical Personal Identification Number (PIN) to complete the authentication process.

Once the user is registered and the BIO+PIN four digit numerical PIN is created access will be validated and the user will be granted access to the computer system for normal operations. Each participant will attempt to authenticate up to five times. Upon successfully authenticating the participants will complete several assigned tasks, logging onto a website and browsing, using a standard Microsoft Office application and sending an email to the principal investigator at rbatie@verizon.net email address with any comments on their logon session experience and logging out of the application.

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 9



What will the Participants do?

Participants on the BIO PIN Study will meet four times during the study
Use the created credentials to:

- Login and use the internet to access the BIO-PIN website and send an email to rbatie@verizon.net This will help determine which authentication method is easier to remember over a period of time (10 weeks)

First meeting Week 1 is registration and Information gathering from each participant:

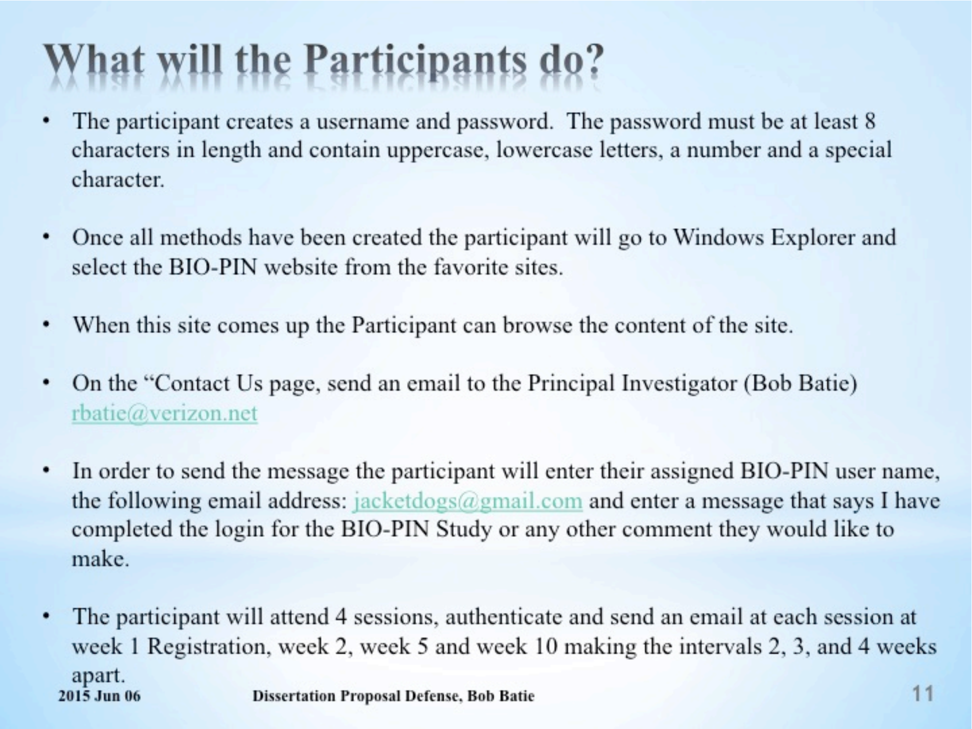
Fingerprints from one hand establishes the BIO-PIN sequence and BIO+PIN Account
Other data collected at that time are:

- Age
- Gender
- Volume (number) of computer accounts
- Frequency of IT usage

The participant will create the BIO-PIN Sequence first by swiping the fingerprints on the fingerprint reader up to 3 times until each fingerprint is accepted and selecting the BIO-PIN fingerprint order. Which finger they will enter first, second, third and last.

The user creates the BIO+PIN using the existing fingerprints and creating a PIN

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 10



What will the Participants do?

- The participant creates a username and password. The password must be at least 8 characters in length and contain uppercase, lowercase letters, a number and a special character.

- Once all methods have been created the participant will go to Windows Explorer and select the BIO-PIN website from the favorite sites.

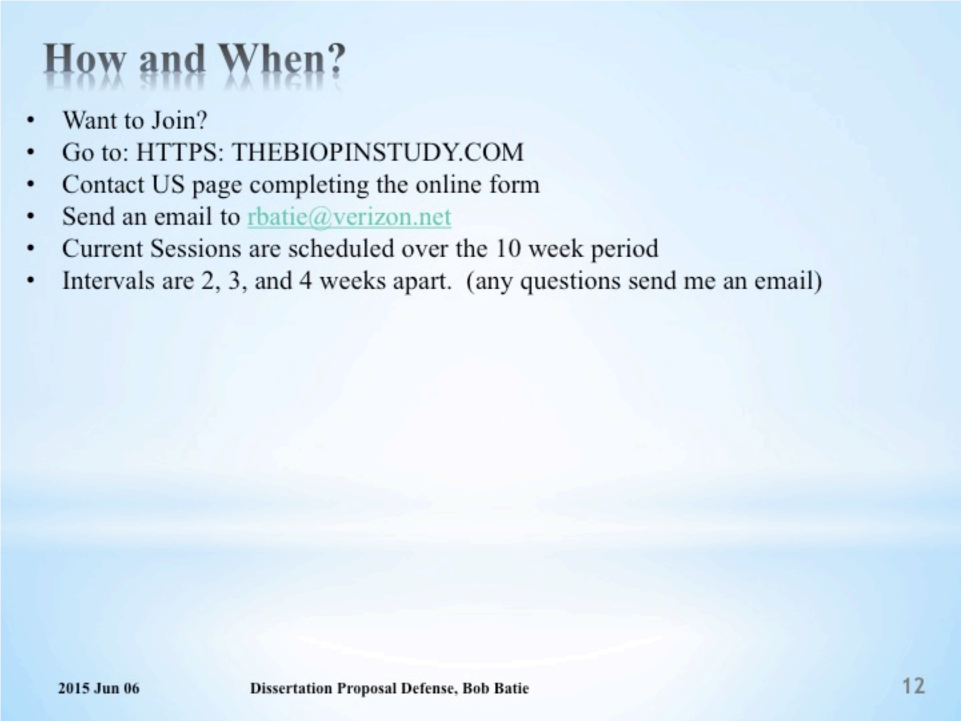
- When this site comes up the Participant can browse the content of the site.

- On the "Contact Us page, send an email to the Principal Investigator (Bob Batie) rbatie@verizon.net

- In order to send the message the participant will enter their assigned BIO-PIN user name, the following email address: jacketdogs@gmail.com and enter a message that says I have completed the login for the BIO-PIN Study or any other comment they would like to make.

- The participant will attend 4 sessions, authenticate and send an email at each session at week 1 Registration, week 2, week 5 and week 10 making the intervals 2, 3, and 4 weeks apart.

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 11



How and When?

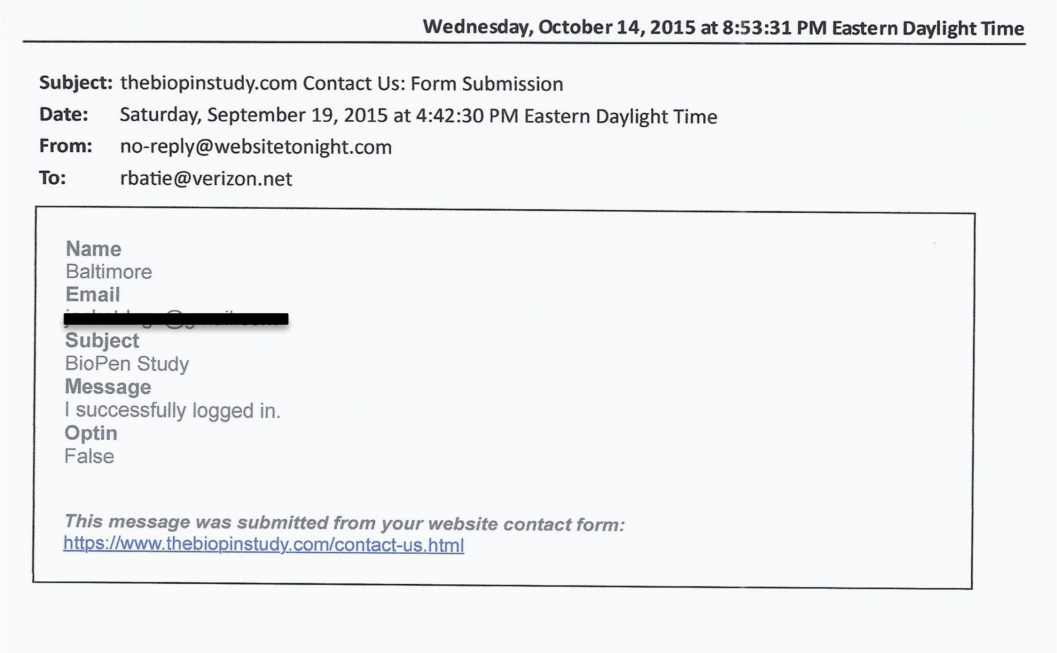
- Want to Join?
- Go to: HTTPS: THEBIOPINSTUDY.COM
- Contact US page completing the online form
- Send an email to rbatie@verizon.net
- Current Sessions are scheduled over the 10 week period
- Intervals are 2, 3, and 4 weeks apart. (any questions send me an email)

2015 Jun 06 Dissertation Proposal Defense, Bob Batie 12

APPENDIX C

Sample BIO-PIN™ emails

This Appendix provides samples of BIO-PIN™ emails sent to the users after accessing the Internet and sending an email to the research team. These samples were randomly selected and cover all login sessions.

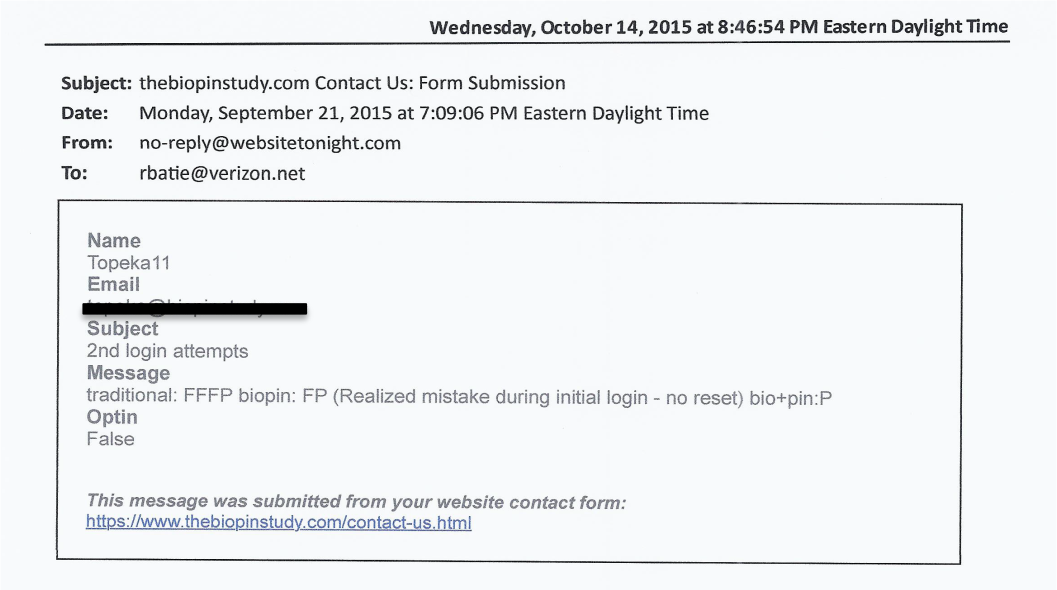


Wednesday, October 14, 2015 at 8:53:31 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, September 19, 2015 at 4:42:30 PM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
Baltimore
Email
[redacted]
Subject
BioPen Study
Message
I successfully logged in.
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

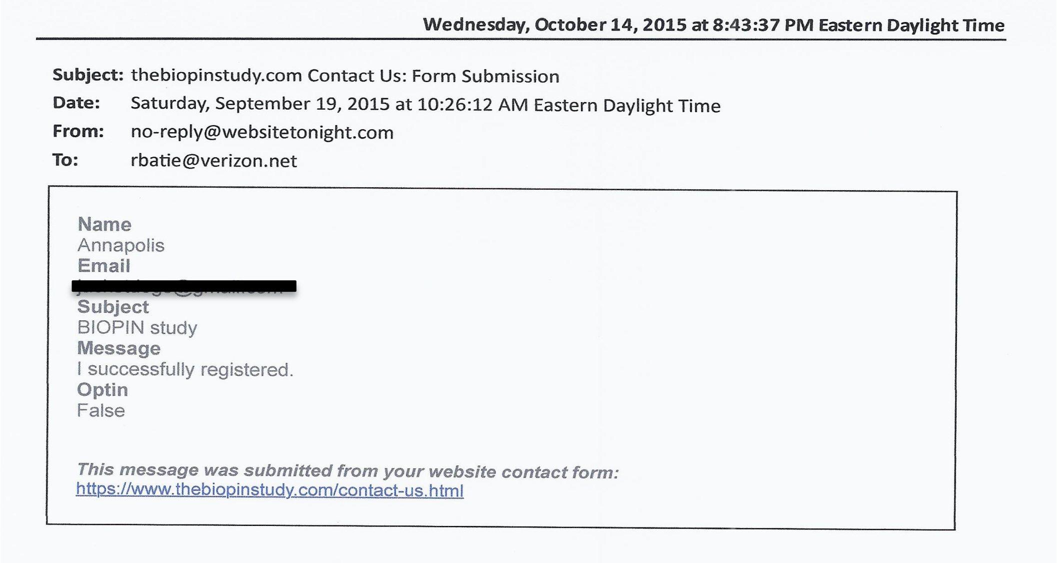


Wednesday, October 14, 2015 at 8:46:54 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Monday, September 21, 2015 at 7:09:06 PM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
Topeka11
Email
[redacted]
Subject
2nd login attempts
Message
traditional: FFFP biopin: FP (Realized mistake during initial login - no reset) bio+pin:P
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

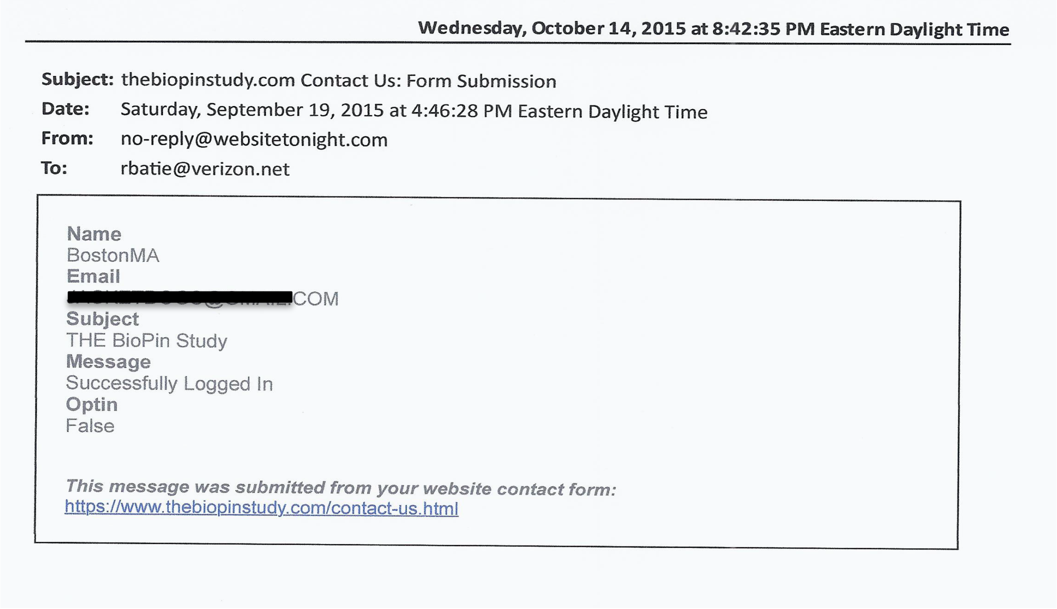


Wednesday, October 14, 2015 at 8:43:37 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, September 19, 2015 at 10:26:12 AM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
Annapolis
Email
[redacted]
Subject
BIOPIN study
Message
I successfully registered.
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

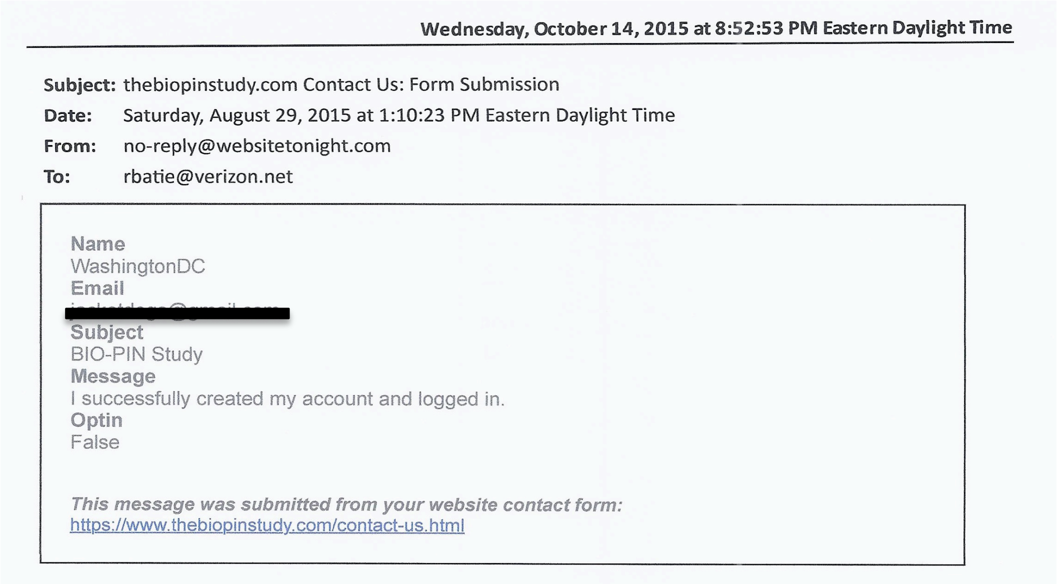


Wednesday, October 14, 2015 at 8:42:35 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, September 19, 2015 at 4:46:28 PM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
BostonMA
Email
[redacted]COM
Subject
THE BioPin Study
Message
Successfully Logged In
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

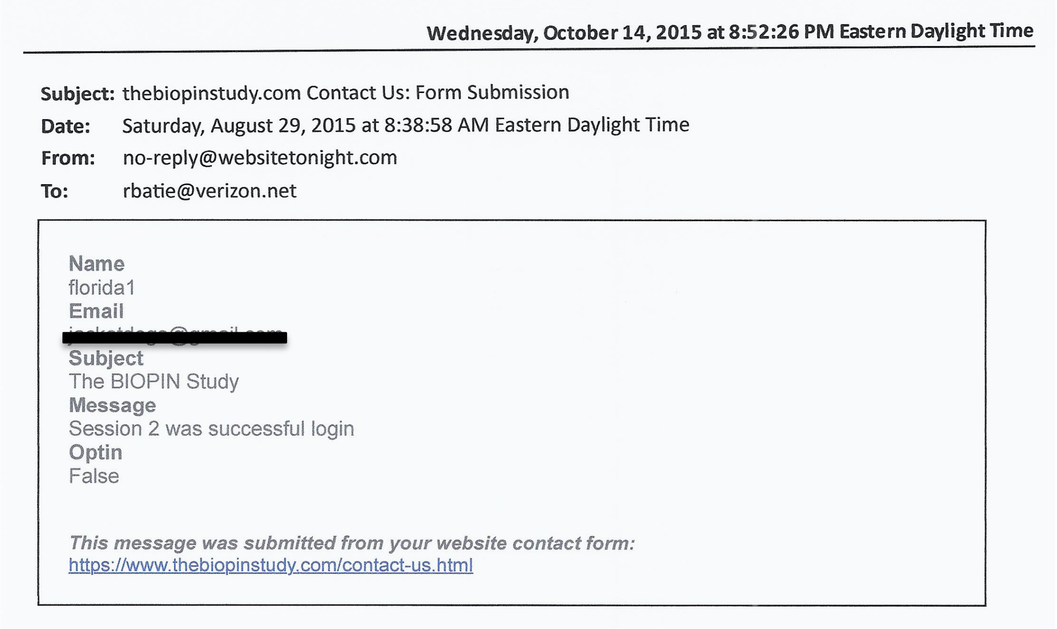


Wednesday, October 14, 2015 at 8:52:53 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, August 29, 2015 at 1:10:23 PM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
WashingtonDC
Email
[redacted]
Subject
BIO-PIN Study
Message
I successfully created my account and logged in.
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

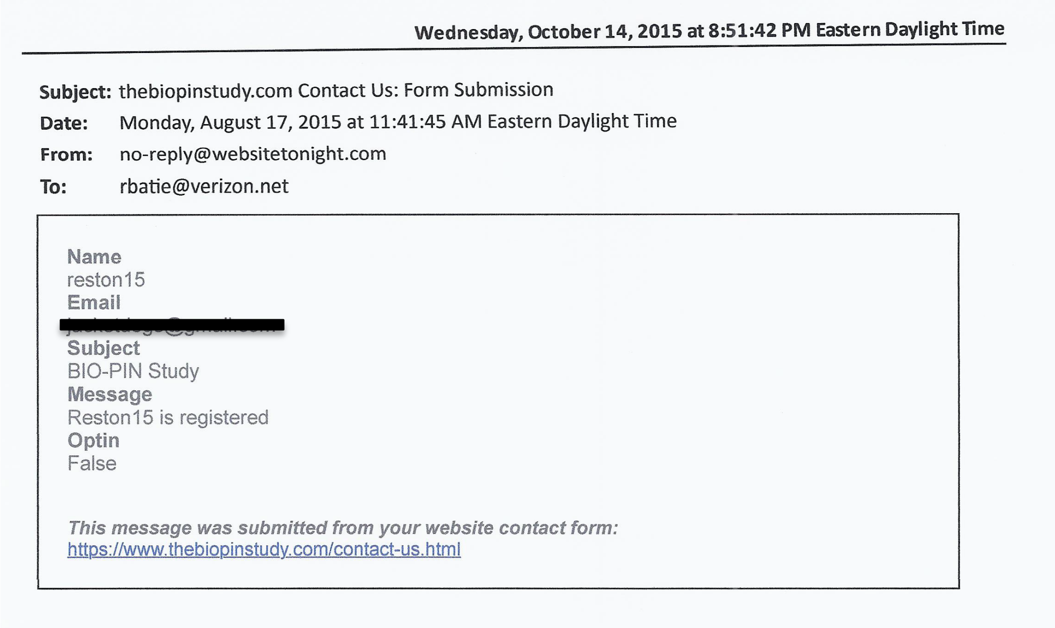


Wednesday, October 14, 2015 at 8:52:26 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, August 29, 2015 at 8:38:58 AM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
florida1
Email
[redacted]
Subject
The BIOPIN Study
Message
Session 2 was successful login
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

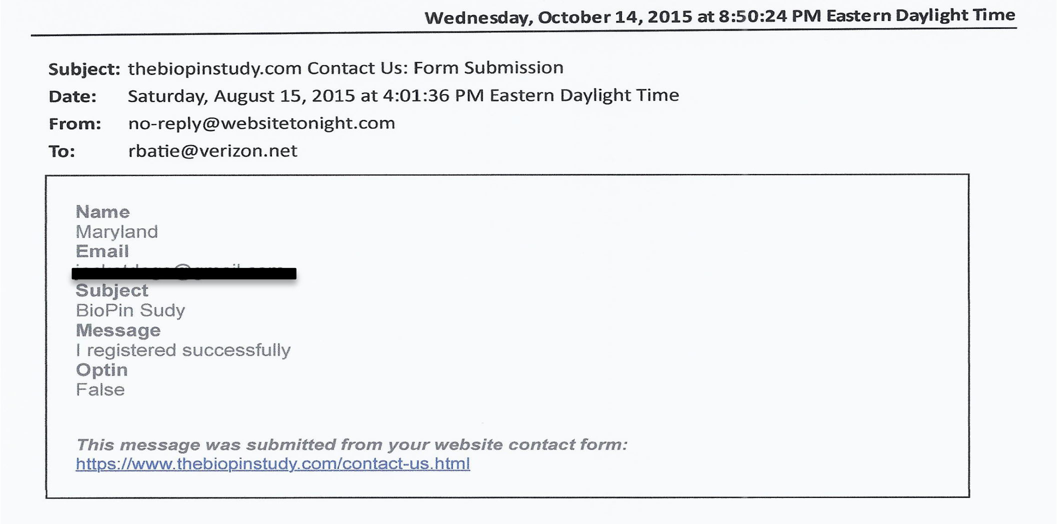


Wednesday, October 14, 2015 at 8:51:42 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Monday, August 17, 2015 at 11:41:45 AM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
reston15
Email
[redacted]
Subject
BIO-PIN Study
Message
Reston15 is registered
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

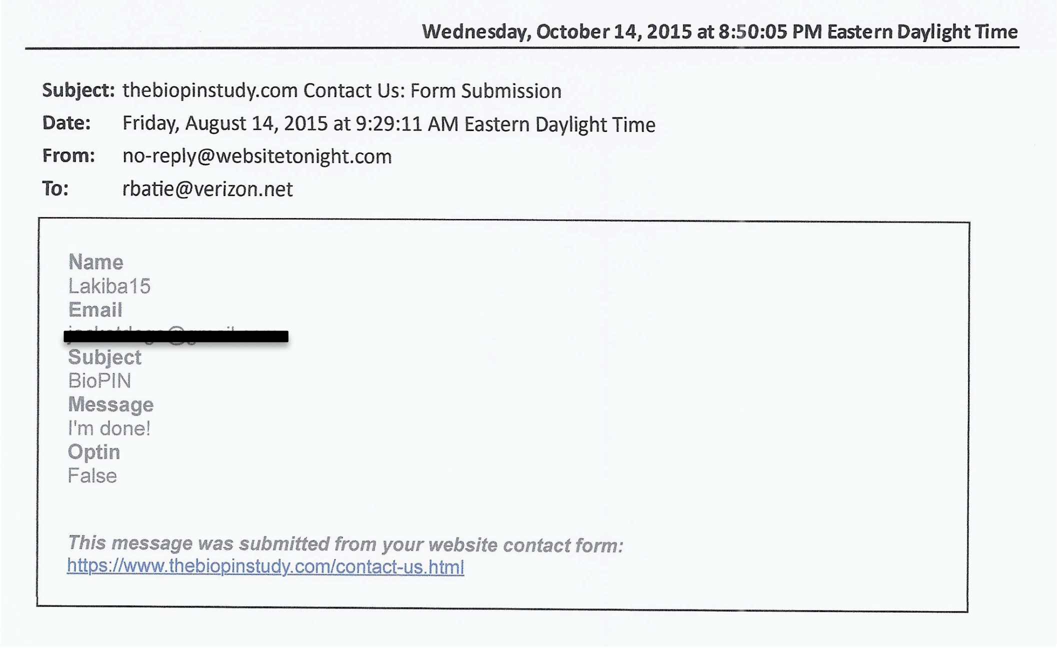


Wednesday, October 14, 2015 at 8:50:24 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, August 15, 2015 at 4:01:36 PM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
Maryland
Email
[redacted]
Subject
BioPin Sudy
Message
I registered successfully
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

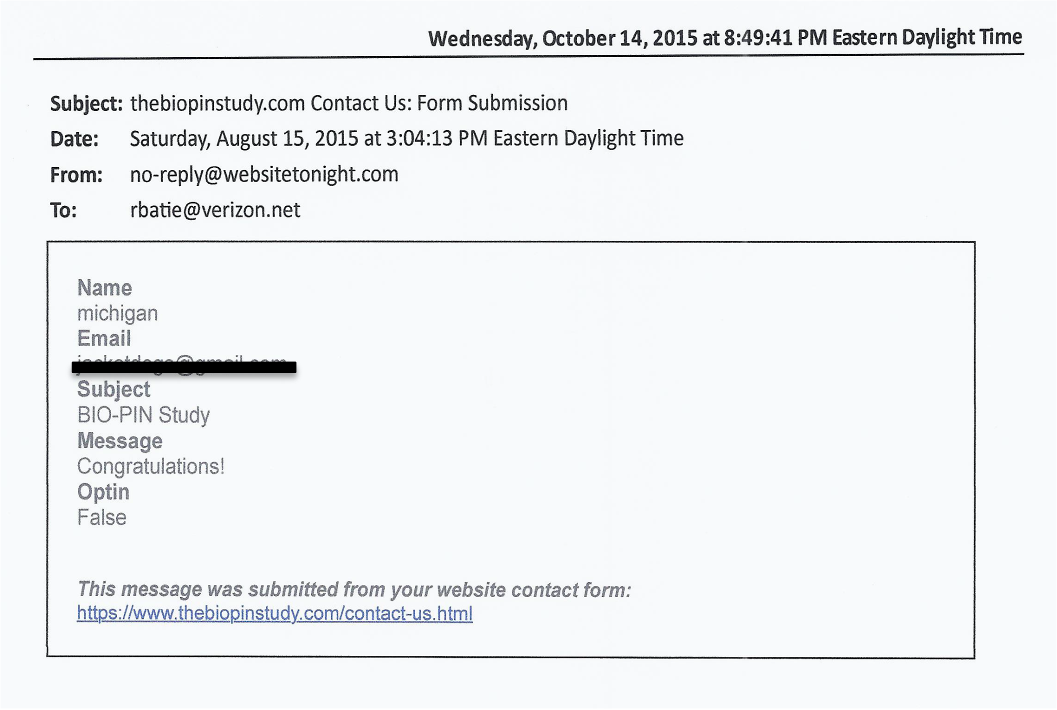


Wednesday, October 14, 2015 at 8:50:05 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Friday, August 14, 2015 at 9:29:11 AM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
Lakiba15
Email
[redacted]
Subject
BioPIN
Message
I'm done!
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html



Wednesday, October 14, 2015 at 8:49:41 PM Eastern Daylight Time

Subject: thebiopinstudy.com Contact Us: Form Submission
Date: Saturday, August 15, 2015 at 3:04:13 PM Eastern Daylight Time
From: no-reply@websitetonight.com
To: rbatie@verizon.net

Name
michigan
Email
[redacted]
Subject
BIO-PIN Study
Message
Congratulations!
Optin
False

This message was submitted from your website contact form:
https://www.thebiopinstudy.com/contact-us.html

APPENDIX D

BIO-PIN$^{™}$ Registration Form

This Appendix is an example of the BIO-PIN$^{™}$ Registration Form used to register participants in the Study. It captures the demographic information and asks the user to document how they create and remember passwords today.

BIO-PIN Study Participant Data Collection

Participants Identification/username	**US State**	**State Capitol**	**Or**	**Major City**
Gender:	**M**	**F**		
Age Group	**18-30**	**31-35**	**36-50**	**51-55**
	56+			
Number of Computer/ Internet accounts	**0-5**	**6-10**	**11-15**	**16 +**
Frequency of computer/ Internet use	**5-8 hours per day**	**2-4 hours per day**	**1-5 hours per week**	

Creating a new password can be difficult. Websites and account management offer suggestions and rules for creating both usernames and passwords such as character length and complexity Industry Standard complex passwords consist of at least 8 characters composed of a capital letter, a number, and/or a special character. Some sites suggest passwords you can choose that comply with their password policy.

1. What is your current method of creating your passwords? (check all that apply)
    a. Using parts of or expanding on a previous passwords
    b. Creating a pass phrase using the first character of each word in the phrase (i.e. from a
    c. book, song title, or bible verse) adding numbers and/or special characters as required.
    d. Creating a pattern on the keyboard
    e. Taking the website or account management suggested password
    f. Other method? Please describe ____
    ____

2. What is your method of remembering your password (password recall)?
    a. Writing it down
    b. Visually recall of the pattern on the keyboard
    c. Association with the type of account you are accessing
    d. Other method? Please describe: ____
    ____

3. After your participation in this Study, which method do you feel was easier to remember?
    a. BIO-PIN™
    b. Username/Password
    c. BIO+PIN

References

Al-Assam, H., Sellahewa, H., & Jassim, S. (2010). Multi-factor biometrics for authentication: A false sense of security. *Proceedings of the 12th ACM Workshop on Multimedia and Security, pp.* 81-88. ACM 978-1-4503-0286-9/10/09

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.

Bolle, R. M., Cornell, J.H., Pankanti, S., Ratha, N. K., & Senior. A. W. (2004). *Guide to biometric,* New York, NY: Springer,

Cavoukian, A. (2005). *Identity theft revisited: Security is not enough.* Retrieved from http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/

Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, *21*(3), 253-265.

Common Criteria Biometric Evaluation Methodology Working Group. (2002). *Common Methodology for Information Technology Security Supplement Version 1.0.* Retrieved from http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf

Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation – design & analysis issues for field settings*. Boston, MA: Houghton Mifflin.

Creswell, J. (2008). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research.* Upper Saddle River, NJ: Pearson Education.

DataGenetics (2012). *PIN Analysis,* Retrieved from: http://www.datagenetics.com/blog/september32012/

Dhamija, R., & 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., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and methods. *Issues in Informing Science and Information Technology, 6*, 323-337.

Erlich, Z., & Zviran, M. (2009). Authentication methods for computer systems security. In Khosrow-PourM. *Encyclopedia of information science and technology.* (Vol. 1, pp. 288- 293). Hershey, PA: Information Science Reference. DOI: 10.4018/978-1-60566-026- 4.ch049

File T. (2013). Computer and Internet use in the United States; Population Characteristics. *U.S. Census. Issued May 2013*. (pp. 20-569). Retrieved from http://www.census.gov/prod/2013pubs/p20-569.pdf

Fogel, J., & Nehmad, E. (2009). *Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior, 25*, 153–160 doi:10.1016/j.chb.2008.08.006

Forget, A., & Biddle, R. (2008). *Memorability of persuasive passwords.* CHI 2008, April, 2008, Florence, Italy, ACM 978-1-60558-012-8/08/04.

Furnell, S. (2007). An assessment of Website password practices. *Computers & Security*, *26*(7 and 8), (pp. 445-451). doi:10.1016/j.cose.2007.09.001

Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000) *Authentication and supervision: A survey of user attitudes, computers and security, 19*(6) 529–539. Retrieved from http://www.sciencedirect.com.ezproxylocal.library.nova.edu

Gaw, S., & Felten E. W. (2006). Password management strategies for online accounts. *Symposium On Usable Privacy and Security (SOUPS) 2006*, Pittsburgh, PA, USA.

Gajek, S., Löhr, H., Sadeghi, A. R., Winandy, M., & Görtz, H. (2009). TruWallet: Trustworthy and migratable wallet-based web authentication. *Proceedings of the 2009 ACM workshop on scalable trusted computing*, 19-28, New York. doi 10.1145/1655108.1655112

Gouda, M. G., Liu, A. X., Leung, L. M., & Alam, M. A. (2007). SPP: An anti-phishing single password protocol. *Computer Networks*, *51*(13), 3715-3726, doi:10.1016/j.comnet.2007.03.007.

Gummesson, E. (2007). Case study research and network theory: Birds of a feather. *Qualitative Research in Organizations and Management,* 2(3), 226-248.

Gutmann, A., Renaud, K., & Volkamer, M. (2015). Nudging Bank Account Holders Towards More Secure PIN Management. In *International Journal of Internet Technology and Secured Transactions* (Vol. 4, No. 2, pp. 380-386). Infonomics Society.

Halderman, A. J., Waters, B., & Felten, E. W. (2005). A convenient method for securely managing passwords. *International World Wide Web Conference Committee*

(IW3C2). WWW 2005, Chiba, Japan. ACM 1595930469/05/0005.

Hasche, S., Berti, J., & Hare, C. (2004). *Official (ISC^2) guide to the CISSP exam.* Boca Raton, FL: Auerbach.

Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: Secure authentication usable anywhere. *Proceedings of the 4th symposium on usable privacy and security*, 35-45. ACM.

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

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., Bolle, R., & Pankanti, S. (1998). Introduction to biometrics. In Jain, A. K., Bolle, R., & Pankanti, S., (Eds.) *BIOMETRICS: Personal identification in a networked society*, 1–41, New York, NY: Kluwer Academic Publishers

Jain, A. K., Flynn, P. & Ross, A. (2008). Handbook of biometrics. In Ross, A., Nandakumar, K., & Jain, A. K., (Eds.) *Introduction to multi-biometrics*, pp. 271-333.

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

Jain, A. J., Hong, L., & Pankanti, S. (2000). Biometrics: Promising frontiers for the emerging identification market. *Communications of the ACM*, 91–98.

Lemos, R. (2013). *iPhone 5S TouchID fingerprint sensor fooled by copied prints.* eWeek Posted 2013-09-26. http://www.eweek.com/mobile/iphone-5s-touchid-fingerprint-sensor-fooled-by-copied-prints.html

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided versus vendor-provided multi-biometric authentication in online exams. *Campus-Wide Information Systems, 28*(2), 102-113. doi:10.1108/10650741111117806

Mallow, C. (2007). Authentication methods and techniques. *Global Information Assurance Certification. http://www.giac.org/resources/whitepaper/access/2.php*.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of fingerprint recognition*, New York, NY: Springer.

Mansfield T., & Roethenbaugh, G. (1999). 1999 glossary of biometric terms. *Association for Biometrics (AfB) and International Computer Security Association (AfB, ICSA).* http://biometrics3.tripod.com/pubs/glossary.pdf

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. *Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, 4677, pp. 275-289.

Maty´aˇs, V., ˇ R´ıha, Z (2010). Security of biometric authentication systems. *Proceedings of the Computer information systems and industrial management applications (CISIM) International Conference,* pp. 19-28, Krackow, Poland. Doi.10.1109/CISIM.2010.5643698,

Maty´aˇs, V., ˇ R´ıha, Z. (2000). *Biometric authentication systems*. Technical report. http://www.ecom-monitor.com/papers/biometricsTR2000.pdf.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*, Boca Raton, FL: CRC Press.

Menkus, B. (1998). Understanding the use of passwords. *Computers & Security*, *7*(2), 132-136.

Mertler, C., & Vanatta, R. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation* (4^{th} ed.). Los Angeles: Pyrczak.

Mertler, C. A., & *Vannatta, R. A. (2013). Advanced and multivariate statistical methods (5th ed.): Practical application and interpretation*. Glendale, CA: Pyrczak Publishing.

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

Mujeye, S., & Levy Y. (2013). Complex passwords: How far is too far? The role of cognitive load on employee productivity. *Online Journal of Applied Knowledge Management, 1*(1), 122-132

National Institute of Standards and Technology (NIST) Special Publication (SP)-800-118, *Guide to Enterprise Password Management.* April 2009

Newbold, R. D. (2008). *Newbold's biometric dictionary for military and industry: 2nd Edition.* Bloomington, IN: AuthorHouse

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics. *Proceedings of the*

IEEE, pp. 2019-2040, Avaya Labs, Basking Ridge, NJ, USA

Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. *Proceedings of the 9th ACM conference on computer and communications security, pp.* 161-170. Washington, DC, USA. ACM 1-58113-612-9/02/0011

Prabhakar, S., Pankanti, S., & Jain, A. (2004). Biometric recognition: Security and privacy concerns. *IEEE Computer Society,* pp. *1540-7993/03*

Raja A. Y., & Arumuga Perumal, S. (2013). Effective method of Web site authentication using fingerprint verification, *International Journal of Computer and Electrical Engineering, 5*(6), 545-548. DOI: 10.7763/IJCEE.2013.V5.769

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems journal*, *40*(3), 614-634.

Ratha, N.K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. *Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228, Heidelberg, GE

Riege, A. M. (2003). Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase. *Qualitative market research: An international journal*, *6*(2), 75-86.

Ren, X., & 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), 23(4)*, pp. 20-24. Poznan, Poland.

Ross, A.A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of multi-biometrics*. New York, NY: Springer.

Salkind, N. J. (2009). Exploring research (pp. 243–251). *Saddle River: Pearson Education.*

Schneier, B. (1999). The uses and abuses of biometrics. *Communications of the ACM, 42*(8), 136-136.

Shenk, M. (2007). Who can you trust? *Computer Weekly, vol 50*, 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. In Chander, A., Gelman, L., & Radin, M. J., (Eds.) *Securing privacy in the Internet age* (pp. 111- 136). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=583483, Jan 26, 2013

Steckler, A., & McLeroy, K. R. (2008). The importance of external validity. *American Journal of Public Health*, *98*(1), 9-10.

Suna, Z., Paulino, A., Feng, J., Chai, Z., Tan, T., & Jain, A. K. (2010). A study of multi-biometric traits of identical twins. *Proceedings of the SPIE, Biometric Technology for Human Identification VII*, *7667*, 76670T-12. Retrieved from www.citeulike.org/user/vipin255/article/8386459

Tognazzini, B. (2005). Design for usability. *Security and usability: designing secure systems that people can use, O'Reilly, Sebastopol, CA*.

Tipton, H., & Krause, M. (2012). *Information security management handbook 2011 Edition*. CRC Press Taylor & Francis Group, Boca Raton, FL

Tullis, T. S., and Tedesco, D. P. (2005) *Using personal photos as pictorial passwords.* CHI 2005 Conference on Human Factors in Computing Systems, Portland, Oregon, USA, April 2-7, 2005. Pages 1841-1844 doi>10.1145/1056808.1057036

Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: A case study in fingerprints. *Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents VI, 622*, San Jose, CA. doi:10.1117/12.530907

Uludag, U., Ross, A., & Jain, A. K. (2004). Biometric template selection and update: A case study in fingerprints. *Pattern Recognition*, *37*(7), 1533-1542.

Vetter, R. (2010). Authentication by biometric verification. *IEEE Computer Society, 43*(2), 28-29. doi10.1109/MC.2010.31

Vykopal, J., Plesnik, T., & Minarik, P. (2009). Network-based dictionary attack detection. *Proceedings of the International Conference on Future Networks, pp. 23-27, Bangkok,* Doi: 10.1109/ICFN.2009.36

Watson, C., Wilson, C., Marshall, K., Indovina, M., & Snelick, R. (2005). *Studies of one-to-one fingerprint matching with vendor SDK matchers.* NISTIR 7221 April 22, 2005

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005) (Eds). *Biometric systems, technology, design and performance evaluation.* Springer-Verlag London England

Weir, C., Douglas, G., Richardson, T., & Jack M. (2009). Usable security: User preferences for authentication methods in eBanking and the effects of experience, *Interacting with Computer, 22(3), 153-164.* Doi:10.1016/j.intecom.2009.10.001

Woodard D., & Flynn, P. (2005). Finger surface as a biometric identifier. *Computer Vision and Image Understanding, 100*(3), 357-384. doi:10.1016/j.cviu.2005.06.003

Yasu Raja, A., & Arumugaperumal, S. (2013). Effective method of Web site authentication using fingerprint verification. *International Journal of Computer and Electrical Engineering, 5*(6)*,* 545-548.

Zhang, D. D. (2004). *Palmprint authentication.* Norwell, MA: Kluwer Academic.

Zhang, Y., Monrose, F., & Reiter, M. K. (2010). The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 176-186). ACM.