Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 5th, 2017

A Study of Biometric Security Technology Acceptance and Primary Authentication

James Fletcher, Phaedra Howard, Darshit Mody, Ayushi Vyas, and Hugh Eng
Seidenberg School of CSIS, Pace University, Pleasantville, New York

***Abstract*—Advances in biometrics present the possibility of providing robust security and authentication methods compared to traditional password-oriented security measures. Biometric security technology relies on who you are rather than what you know, in contrast with knowledge-based security. While biometrics has the potential to increase security significantly, it also presents unique drawbacks. Addressing these potential problems and increasing the rate of user acceptance are key elements to its success. This research aims to discover the degree of acceptance of biometric security over a wide range of demographics. It considers acceptance levels and their relation to perceived usefulness and perceived ease of use. Additionally, it analyzes important acceptance factors such as social, organizational, and cost concerns. Finally, it presents conclusions on biometric security acceptance in general and as a primary authentication method relative to age, income and education level**.

Keyword Terms: Biometrics, Ease of Use, Identity Authentication, Information Security, Technology Acceptance, Security Fatigue

I. INTRODUCTION

This paper presents research and conclusions, based on an anonymous survey, regarding the positive aspects of biometric technology acceptance as well as negative issues and concerns. Concentration is on the use of biometrics to replace passwords, usernames, and personal identification numbers as the prevalent form of primary authentication for users of the internet and information technology applications. The survey aimed to test the hypothesis that the degree of acceptance tends to be higher for users who are younger, are more educated, and have incomes at or above current median levels [17]. This paper also presents suggestions for overcoming some of the obstacles to acceptance.

Many people today have to manage a large number of accounts and corresponding security usernames, passwords, and PINs (personal identification numbers) that rely on uniqueness for their security. This can be overwhelming, and some users experience what can be referred to as security fatigue [16]. Shortcuts and repeated use of the same words and phrases defeat the purpose of uniqueness and substantially reduce security.

Information such as bank-account, credit-card, and health data are increasingly vulnerable using traditional password methods. This is especially relevant in 2016, as the incidence of information theft is rising sharply, and technology such as the Internet of Things has the potential to add literally billions of connected devices to the internet. Gartner, Inc. forecast that "6.4 billion connected devices will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020. In 2016, 5.5 million new devices will get connected every day" [7].

The use of personal passwords and PINs remains the primary source of security for these applications and devices. Due to the sheer number of sites and systems requiring passwords, many users resort to simple, easy-to-remember passwords that provide an easy target for hackers. As Darlene Storm noted in a January 2016 *Computerworld* article [24], yearly studies by the company SplashData show that the most popular passwords—such as "123456," "password," and "abc123"—are weak, easily guessable, and put users at extreme risk for hacking and identity theft. Major websites such as Amazon, Facebook, Twitter, and LinkedIn—representing more than 2 billion active users in 2016 [1]—require a six-character minimum as the only password creation limitation. The weak, easily cracked passwords mentioned above are all completely acceptable on these sites.

User acceptance of biometric security devices and applications such as fingerprint-, iris-, voice-, and vein-scan recognition can significantly increase security over password use. These types of biometric applications are currently available for use in devices such as mobile phones, laptop computers, and company security systems.

Using results from an online survey, this paper examines data on how extensively these biometric devices are being adopted and accepted. Some of the general concepts considered are: Does using biometric security seem easy and convenient? Is there a bias against or an aversion to biometrics? Is there a personal bias against new technology? Is biometric security perceived to be personally intrusive or an invasion of users' privacy? Do cultural or religious conflicts exist regarding the use of biometrics as a method for authentication of identity?

This paper examines the hypothesis that the majority of the survey respondents who are under age 40, have an income at or above median levels [17], and have at least some college education will be much less apprehensive about adopting the use of biometric security features. It aims to identify the main issues that cause the most skepticism and isolate those specific concerns that might hinder or impede an individual's willingness to use biometric interaction for security and authentication purposes.

This paper is a continuation of work done previously by Pace University students on biometric security acceptance. In the paper "A Biometric Security Acceptability and Ease-of-Use Study on a Palm Vein Scanner" [19], research showed the factors of acceptability and examples of flaws in traditional security applications such as passwords. That paper discusses the need to safeguard the vast amount of sensitive data that can be collected and makes evident the related risks and concerns. Its authors present pros and cons of traditional biometrics systems. Their research found that palm vein scanning provided significant advantages over the limitations of some applications, such as fingerprint scans. A survey that was part of the research showed positive acceptability ratings for biometrics and the palm vein scanner.

Of particular note was the fact that 90% of those taking the survey responded positively to the question of whether biometric technology will become one of the dominant authentication methods used in the future [19]. However, concerns about intrusiveness, privacy, and data security are also evident. This data points to the idea that people know the widespread use of biometrics is coming but still have concerns as to its use and safety. This paper continues and expands on these concepts of biometric security acceptance with a new survey.

The first section of this paper describes the methodology for the research. The second section provides a literature review of past studies on biometric acceptance. Further sections discuss the drawbacks of usernames and passwords as a primary source of authentication, and the prevalence of security fatigue among those who have to use them. Finally, an analysis of the survey results and conclusions are presented. Suggestions for overcoming some of the objections to biometric security acceptance and possible methods to increase it are discussed, leaving open potential future research on the subject.

II. METHODOLOGY

This study makes use of quantitative research methodology, applying statistical and numerical analysis to data collected through an anonymous online survey. The survey gathered basic demographics about respondents, such as age, income, occupation, and gender. It also asked respondents about their personal username and password habits, and the number of accounts they manage, in order to facilitate analysis of security concerns. The survey also included questions specific to biometric security acceptance. The following inquiries were highlighted in the survey:

"Do you consider biometric security applications to be an invasion of privacy and, if so, for what reasons?"

"Would you consider using a single biometric security application or device to replace frequently used passwords and/or personal identification numbers?"

Questions to ascertain the degree of acceptance due to perceived ease of use, perceived convenience, and factors such as increased security were included, as were questions about awareness of and experience with specific biometric security applications such as facial recognition, eye recognition, and fingerprint scans. Full text of the survey questions is included in *Appendix A*.

Additional methods deployed for the survey:

A. Determining Sample Size

Achieving a mathematically derived minimum survey sample size is required to raise confidence in the integrity of the data analysis results. Equations were used to calculate how many responses would be necessary to make the survey efforts relevant and credible.

Previous research points to statistical knowledge as a requirement to come up with the correct sample size. In his article "Determine Sample Size: How to Ensure you get the Correct Sample Size," Scott M. Smith, Ph.D. [21], lists four criteria needed to make this determination: population size, margin of error (confidence interval), confidence level, and standard of deviation. By estimating the approximate number of people who fit the desired demographics and setting a plus-or-minus percentage margin of error, a 95% confidence rate is attained. Using 0.5 as the standard of deviation, approximately 384 samples were needed to reach the survey goal. The desired confidence level corresponds to a Z-score found in a chart included by Smith. Since a 95% confidence level was desired, the Z -Score = 1.96. The Z-score, standard of deviation, and confidence interval fit into the equation as follows:

$$\textit{Necessary Sample Size} = (\textit{Z-score})^2 * \textit{StdDev}*(1-\textit{StdDev}) / (\textit{margin of error})^2$$

For this survey, the inputs to the equation were at the 95% confidence level, 0.5 standard deviation, and a margin of error (confidence interval) of +/- 5%. This is represented in equation form as:

$$((1.96)^2 \text{ x } 0.5(0.5)) / (.05)^2$$

$$(3.8416 \text{ x } .25) / .0025$$

$$.9604 / .0025$$

Totaling 384.16

This calculation determined that 384 survey responses were needed to reach the desired 95% confidence rate goal for this study.

B. Validation Survey Questions

In addition to determining sample size, it was essential to establish a method of validating that the respondents were focusing on each question and not just clicking through or selecting random answers. This activity tends to produce unreliable data. Using the information on ways to ensure valid survey responses in another article by Smith [22], the survey incorporated certain questions to ensure the data from responders would be reliable. One of the methods Smith suggests is using a "trap" question. This method presents an obvious question with an obvious answer that might be missed by someone not paying attention or moving too fast to supply reliable data. The trap question used in this survey was *"If you live in the U.S., select Strongly Agree"* followed by *Disagree, Agree, and Strongly Agree*. It could be ascertained that respondents residing in the U.S. who chose anything but "Strongly Agree" as an answer might not have been paying close attention and might have provided invalid or unreliable data.

Another validation technique suggested by Smith involves what he refers to as reverse wording. With this method, the same question is asked twice, first as a positive and second as a negative. In this survey, a reverse wording question was added that asked: *"Please rate yourself based on the following statement: "I consider myself to be an early adopter of new technology."* Rating options followed. Later in the survey, respondents were asked, *"Please rate yourself based on the following statement: I consider myself* ***not*** *to be an early adopter of new technology."* The same rating options followed. Observing whether the respondents gave equivalent answers to both questions helped determine their attention span while taking the survey and thus the relative validity of all of the answers they provided.

C. *Determining Income*

The survey attempted to see how income relates to levels of biometric security acceptance. According to the American Community Survey conducted by the U.S. government and published on Census.gov, the median household income for Americans in 2015 was $55,575 [4]. For this survey, this number was rounded to $56,000 and then used as the median. To choose the levels and break-off points for classifications such as lower class, middle class, and upper class, data from Pew Research was used. According to Pew, "middle-income Americans are adults whose annual size-adjusted household income is two-thirds to double the national median. Lower income households have incomes less than two-thirds of the median and upper-income households have incomes that are more than double the median" [17]. Questions about income levels and the number of contributors to a household were asked using this data as a reference.

D. *Survey Distribution and Opt-Out Options*

The survey was distributed by anonymous link using social media such as LinkedIn and Facebook, as well as direct requests to family, friends, and colleagues to obtain as many survey responses as possible across a wide range of demographics.

The survey included an opening statement: *"This survey is built using an anonymous link, which does not collect or retain any personal data such as name, email address or IP address. It only retains the responses you provide. These are given a unique anonymous identifier based on the date they are recorded. Your answers will be used for a project and dissertation on consumer acceptance of biometric security technology. This information will be retained in its anonymous format by Pace University for future education projects."* This is followed by an option to continue the survey or opt out and provide no data. This statement is to assure respondents about the safety of their data so that they might not be discouraged from taking the survey if this was an initial concern. It also aided in filtering out respondents who may have provided unreliable data based on this concern by giving them an option to end the survey before entering any answers.

III. LITERATURE REVIEW

There has been much study on the usage of biometric devices and applications, users' attitudes toward such devices, and measurements of impact on performance. Performance gains are often the most significant incentive for adopting a new technology. In relation to this study, the use of biometrics in place of the commonly used passwords could potentially increase performance and security, but user acceptance is the key to its success. As Davis has noted, "Although actual organizational performance gains are the desired outcome from the use of new information systems, these gains will not be obtained if users fail to adopt the new system. The actual use or non-use of an information system is an important and overlooked issue in the design and selection of information." [3] The usefulness and perceived ease of use of a new technology will have a great impact on how quickly users are willing to adopt it. People will have different specific needs from a system or device that will influence its perceived usefulness. Potential users may also have different experience and ability levels with a particular device. This will have an effect on its perceived ease of use.

With innovative technologies such as biometrics, user acceptance needs to be an equally important factor as usefulness and convenience. Acceptance is also more complex than perceived usability, as it involves social, organizational, and cost factors. Many people have an aversion to learning and accepting new technology or may consider it too inconvenient. Hee Cheol Kim [10] suggests that innovative and new technologies tend to be intrinsically inconvenient. Therefore, it is important to consider acceptance factors in addition to perceived usability, ease of use, and performance gains when designing a new technology or device.

Until recently, not many studies had been performed to evaluate innovative technologies from a user acceptance perspective. In response to this deficit of knowledge, a new discipline has been established, the study of Acceptability Engineering (AE) [10]. It is an academic field that explores theories and methods for acceptable innovative technology design, and attempts to identify differences between Human Computer Interaction (HCI) and Acceptability Engineering. This, in turn, reveals a difference between usability and acceptability and better defines the scope of acceptance engineering. These techniques are helping to define and clarify characteristics needed to understand user acceptance.

Continued research has found a relationship between user acceptance of a device or system and the role potential users have in its development. If users have an important part in the design and proposed functionality of biometric interaction, acceptance will be higher. A company may be more successful in getting employees to accept a biometric security device if it invests resources in obtaining employee input. This ultimately helps facilitate the feasibility, functionality, and acceptance of a biometric device as part of the successful implementation of an overall security plan.

Data from the biometric security acceptance survey conducted for this paper provides insight on how these acceptance factors relate to biometric security among different demographics.

Another potential barrier to acceptance of biometric devices and systems is the perception that they are too intrusive compared to using personal passwords. Biometric security is based on *who you are physically*, rather than *what you know*, which is fundamental to its heightened security potential. However, some people feel that allowing a device to "read" their physical person is providing too much information that is not necessary and could potentially fall into the wrong hands for subversive or illegal purposes.

Kat Krol et al. [12] performed a study on facial recognition biometrics as an alternative to the CAPTCHA matching system used by many online ticket sites to determine whether a transaction is conducted by a human or a "bot." CAPTCHA is a favored device used by ticket agencies to prevent unauthorized mass purchases of tickets that could later be "scalped" for much higher prices. Study respondents expressed concern that someone might see their picture, or that they could be identified based on that picture. Some participants indicated that any security gain that facial recognition may have provided was not worth the loss of privacy, that having their picture taken was intrusive, and that they were concerned their data could be used for potentially illegal activity. The survey conducted as part of this research paper asked questions about these types of privacy concerns and sought to determine whether they are associated with particular demographics.

Social and cultural concerns can be another barrier to biometric technology acceptance. In some areas of the world, it is common to avoid any publicly used device, such as a biometric fingerprint scanner. In a cultural study of biometric use, Rashed et al. [18] found that the majority of Arab respondents were willing to provide information such as personal passwords, fingerprint scans, and PINs. However, for certain Asian respondents, the willingness to provide this type of information was below 50%, especially with scans of physical or personal characteristics such as voice recognition. In America, Amish communities are culturally and religiously opposed to technology. State requirements to have pictures on their driver's licenses or traffic safety devices on their horse-drawn carriages have proved a challenge. In a European study, Krupp et al. [13] concluded that users tended not to see big advantages of biometrics over authentication mechanisms such as passwords and PINs, despite improved security. They found that general awareness regarding biometrics needs much improvement, which may also drive more widespread social acceptance of the technology.

Abed et al. [5] have highlighted several points in their study of user acceptance and how it relates to satisfaction with biometric systems. They found that the number of various uses and the information provided by the biometric devices relates directly to how well it is accepted. In their study, there was also concern that personal data (i.e., the biometric template) could be misused to gain access to sensitive private data, and once the biometric template as stolen, it is compromised forever. The possibility of stalking or assaulting individuals to steal their biometric information could also prove problematic. Also, the issues of hygiene and direct contact with biometric devices presented potential barriers. In particular, a survey of military aviators expressed concern among respondents that a retinal or fingerprint scan might damage their eyes or hands if used long term, putting their skills at risk. Results of the biometric security acceptance survey conducted for this paper sought to discover the factors behind this possible reluctance to accept biometric security.

In the efforts to replace passwords with biometrics, a new product being tested by Google under the title Project Abacus [14] is of particular note. Initially using the Android mobile platform, Abacus attempts to use the existing technology built into a mobile device to work with its biometric application to provide authentication. Since smartphones already inherently have the ability to sense inputs such as voice, fingerprint, and text as well as the capacity to determine your physical location and surroundings, Abacus presents the software to use these for authentication purposes. By tracking physical traits and combining them with real-time statistics such as geographic location, Abacus will develop what it calls a "trust score." Based on the trust score, the application will authenticate the user or lock them out. Varying degrees of trust scores are applied to different applications requiring different levels of security. For instance, a simple game may require a lower trust score than a secure banking system where more is at risk.

Google is attempting a significant step in tackling the issue of using secure biometrics to completely replace users' responsibility of utilizing PINs and passwords for authentication. Many countries and leading technical universities are helping to participate in this venture, and beta testing is occurring in the second half of 2016 with several banking institutions. How well this technology will be accepted and how well Google has considered the end-user experience remains to be seen. Google's Chrome browser is notorious for using up battery power much faster than other browsers, such as Firefox and Edge [15]. Abacus may present a similar problem for Google, since the biometric scanning, and geographic tracking all require constant battery use. End users may be unwilling to use a biometric application such as Abacus if it is going to significantly drain the battery life of their device and cause the inconvenience of more frequent battery charging.

The problem of adapting biometric security for people with special needs, such as the elderly or disabled, is also an issue affecting their levels of biometric security acceptance. If a person is unable to display or access some of the required traits for the biometric security device due to physical limitations, this could negatively affect their ability to use it at all. Further, if a person is incapacitated for some reason, friends, relatives, or emergency and health workers may need to access their information and would be unable to. In his paper "Biometric Authentication for Older Adults" [11], Kowtko describes some of the problems traditional security applications such as passwords pose for the elderly due to issues such as gradual memory and mobility loss. Biometrics is frequently being considered by health professionals and institutions as an alternative to passwords, but the issue of its ability to safely guard personal data and to be used as a sole authentication method for older adults is brought into question. Per Kowtko, "Biometric Systems should be utilized as a supplemental authentication. It should not replace a smart card, username, or another credential that requires a user to either 'have' or 'know' something."

Security concerns with biometrics remain a possible barrier. Some experts on the topic say that biometrics are intrinsically secure, since no one else can have your unique physical characteristics. "Alvaro Bedoya, Professor of Law at Georgetown University, argues otherwise. A password is inherently private. The whole point of a password is that you don't tell anyone about it. A credit card is inherently private in the sense that you only have one credit card. Biometrics, on the other hand, are inherently public" [8]. A picture can be taken from afar to replicate a face, or a fingerprint could be lifted from a glass to replicate it. This makes them easy to hack and easy to track.

The issue of resetting a biometric profile is also a concern. We can reset passwords as often as needed, but we only have one set of eyes, ears, and fingerprints. Resetting a profile may mean accessing the profile in a stored database. These databases are as vulnerable to hacking and compromise as any other server containing passwords to financial or personal data used by companies, but in this case, the consequences are more severe. Companies will need to go through great effort to assure users that their data is encrypted and safe in order to give the technology a better chance to be widely accepted.

Use of an individual's biometric data is relatively unregulated. Laws restricting government access to personal data on devices versus the need for this data for national security purposes are still being debated, and this problem is amplified with biometrics. This issue will have to be resolved not just in the United States, but globally.

A. Security Fatigue

"Security fatigue" can be defined as "a weariness or reluctance to deal with computer security" [5]. Warnings of imminent threats posed by cyberattacks and the methods needed to protect themselves can overwhelm some users. This includes the need to change and create new passwords that won't be easily guessable or hackable; the need to remember and manage those passwords; and paying for, installing, and updating antivirus and spyware protection. Eventually, users reach a saturation point and begin to become immune to the issue of cybersecurity. Per Furnell et al., "there is a threshold at which it simply gets too hard or burdensome for users to maintain security. This makes people desensitized and weary" [5].

Security fatigue is also closely linked to decision fatigue. If faced with too many possibilities, an individual can be driven by impulse into selecting what is easiest rather than what is to their best benefit.

"Manifestations of security fatigue as a specific example of decision fatigue include:

- avoiding unnecessary decisions,
- choosing the easiest available option,
- making decisions driven by immediate motivations,
- choosing to use a simplified algorithm,
- behaving impulsively, and
- feeling resignation and a loss of control" [15].

In their study on security fatigue, Stanton et al. note that "Users feel inundated by the tasks, choices, and work that security decisions require of them and are unsure that compliance actually makes them any more secure. Whatever they do, it is never quite enough. The hackers would always be two weeks ahead of them" [23]. Participants expressed their frustration with comments that no person is safe from a well-planned cyberattack and that if a hacker wants to gain access, they will, no matter how vigilant a user is. They also expressed feelings that they shouldn't have to play such a significant role in their cybersecurity and that higher level organizations such as websites and employers should shoulder most of the burden.

For this study, this relates to using passwords as a primary method of authentication. As minimum requirements for password authentication become more complex on some sites, the chances that a user might make a mistake while entering their password increases. The possibility of their account being locked, requiring a reset and yet another new password, also increases. The annoyance and frustration with password management further leads to security fatigue.

Per Theofanos, the general attitude of users toward cyber security is extremely negative. He suggests that cybersecurity rules be simplified or eliminated to reduce multiple complex decisions for users, thus lowering the risk of long-term security fatigue. He also recommends that companies take a larger role in identifying and controlling these decisions, to make things easier for their users. "Providing individuals with more service and minimum cost for safety against cyber threats and hazards would help balance the bitterness/ negativity in the online environment" [23]. A secure, reliable and proven biometric security device may be the answer to help reduce security fatigue. By eliminating the use of usernames, passwords, and PINs in favor of biometrics, user frustration with this step of the process is lessened, and the threats posed by simple, easily hackable passwords reduced or eliminated. Also, if companies do as Theofanos suggests and contribute more to the responsibility and cost for biometric security, acceptance of the technology should be faster and more widespread.

B. Issues with Password Complexity on Major Websites

Despite the fact that many companies have begun to use minimum password requirements such as 8 or more characters and alpha, number, and special characters, many major websites still have very lax minimum requirements to sign up for their sites. If we focus just on popular sites Amazon, Facebook and Twitter, these sites have a total of over 2 billion user accounts as of April 2016 [1]. All of these have a minimum requirement of just six characters as the only limitation for creating a password [2]. While these companies encourage using a strong password, no special characters, capital letters, or other devices to make it more complex are required. It is in these companies' best interest to make sure their sites are as easy as possible to sign up for and use, but security suffers. As noted above, overly simple and hackable passwords such as "123456" and "abc123" are completely acceptable on Amazon, Facebook, and Twitter.

The online security company Dashlane rated more than 80 popular websites on their password security. More than 85% failed to meet Dashlane's minimum suggested safe password requirements, more than 40% accepted lazy passwords such as "123456" and "password," and half failed to lock accounts after 10 incorrect login attempts [2]. Use of biometric security as an alternative to usernames and passwords for these sites would increase security for their users and lower the amount of security fatigue they might potentially experience.

IV. DATA ANALYSIS

The following is an analysis of the data provided by respondents to the biometric security acceptance survey conducted for this paper in November and December 2016.

A. Demographics

There were a total of 410 respondents to the survey. This number does not include respondents who decided to opt out of providing information after the initial disclosure statement described in the methodology section of this paper.

When asked their gender, 50% identified as male and 49% identified as female, with 1% preferring not to answer. There was an even distribution of ages ranging from 18 to 55 and over, with each category accounting for approximately 20% of the total.

Education levels ranged from some high school or less to professional and doctoral degrees, with 88% having a two- or four-year degree or above. As for occupation, the majority fell into one of two categories; 58% were in managerial/ professional/technical roles, and 20% were in education-related fields, showing a possible correlation with the degree of education received. The remainder were in industrial, health, service, or retail occupations or unemployed.

Approximately 5% of the respondents had an annual income less than $18,000, and 13% ranged from $18,000 to $56,000. As a majority, 57% of the respondents had an annual household income ranging from $57,000 to $200,000, with 59% of the households having two or more individuals contributing.

B. Previous Biometrics Use and Background

Respondents had a wide range of awareness of current biometric security methods. Some 76% had used fingerprint scanning, 33% voice recognition security, 20% eye/retina scans, and 3% behavioral methods such as gait recognition.

Fully 76% of the respondents own a digital device such as a mobile phone, tablet, or laptop with a biometric security device such as fingerprint scan. Of these, 67% used the feature, 27% did not, and 9% stated that they had tried it, but it did not seem to work well. These statistics may point to the problem of awareness and getting users to accept the technology when they first encounter it through simple, reliable, and user-tested processes. The technology may be on a new smartphone, tablet, or laptop. If developers take the time to consider actual user data when designing a biometric security application and make an effort to promote the use in a positive way, awareness and acceptance may increase.

In response to the question “I am an early adopter of new technology,” 74% fell in the range of somewhat to strongly agree, with the remaining 26% in the neutral to strongly disagree range.

C. Perceived Ease of Use, Convenience, and Security

The survey indicates that if a biometric security application is accepted, perceived ease of use, convenience, and security may increase. Fully 87% of respondents stated that they are or might be willing to use a single biometric security application or device to replace the need for multiple passwords, usernames, and PINs. Of these, 65% cited increased ease of use, 64% greater security, and 65% increased convenience. Those who would not consider using it cited the following concerns:

- Risk of having my personal authentication data all in one place: 55%
- Concern that a biometric application or device could be hacked or stolen: 50%
- Safety of my personal biometric data: 44%
- Cost: 22%

Other concerns raised were the inability to dynamically share biometric security with multiple users such as a spouse, concern that a system malfunction could lock out access to all devices or applications, and concern that government agencies could gain or demand access to biometric data.

D. Username and Password Patterns and History

Overall, security is only as effective the weakest link in the security chain. No matter how robust the security plan a company, online service, or home network has in place, if end users are employing simple, easily hackable passwords, they are still vulnerable to attack.

In the survey, 37% of respondents stated that they use simple and easy-to-remember passwords, versus 63% who use difficult ones with long phrases and extra characters. Only 18% reported that they always use a unique password when creating a new one, and 73% reuse the same password and username repeatedly. Some 8% always used the same password for all accounts. Also, 42% responded that they have a minimum of 11 to 30 or more accounts requiring a password. Generally speaking, the results show that more than a third of respondents use passwords that are not unique and are easy to remember versus being secure; they have many accounts to manage, and the majority tend to use the same usernames and passwords repeatedly. Results were similar regardless of demographics such as gender, age, income, and education level. These factors did not make a significant difference in how the respondents use and manage password security.

This data illustrates how password/username preferences can be a weak link in the security chain. A biometric security device or application to replace usernames and passwords would substantially decrease this weak security link through its basic use of who you are rather than what you know.

E. Cost as an Acceptability Factor

Results showed that 22% of respondents considered cost to be a barrier to using a single biometric application to replace usernames, passwords, and PINs. When all respondents were asked if they would be willing to pay out-of-pocket costs for a biometric application or device, 40% stated that they would be prepared to pay between $1 and $10, 8% were willing to pay between $11 and $50, and only 3% were prepared to pay $25 or more. Most importantly, 49% were not willing to pay anything at all for a biometric security application or device. From this data, we can see limits to personal cost that these people are willing to bear. The fact that the majority would be prepared to pay little or nothing points to the issue of companies and developers possibly having to bear the burden of the cost of widespread biometric security acceptance.

F. Intrusiveness and Privacy Concerns

Among survey respondents, 48% said they at least partially considered biometric security scans to be intrusive or an invasion of privacy. Their primary reasons for these concerns were:

- I don’t want to share my personally identifying characteristics: 61%
- I don’t like the idea of being tracked to update or maintain a biometric profile: 52%
- Aversion to physical contact with the device, especially if shared/public: 28%
- Social, cultural, or religious reasons: 12%

These drawbacks need to be considered to promote wider acceptance of biometric security. End users need to know their biometric data is safe and kept completely private. More widespread use of biometrics such as voice and gait recognition that can scan but don't require physical contact may also increase acceptance for those who have a physical aversion to contact with a device.

G. *Hypothesis Test*

In a test of the hypothesis that acceptance of biometric security will be higher with people who are younger, more educated, and of higher income levels, the survey data shows the following for the 40% of respondents in the 18-40-year-old range:

- 62% are in the $56K–$200K+ income range. This is at or above the median levels for middle and upper income for both single earners and multiple-earner households.
- 86% had at least a 2- to 4-year college education.
- 74% considered themselves early adopters of new technology, somewhat agree to strongly agree.
- 67% currently use a biometric security feature.
- 51% said they would consider using a single biometric feature to replace passwords.

The survey data shows the following for the 60% of respondents in the 41-year-old and older range:

- 87% are in the $56K–$200K+ income range. 43% are in the $121K–$200K+ range, which is well above the median levels for middle and upper income for both single earners and multiple-earner households.
- 88% had at least a 2- to 4-year college education.
- 74% considered themselves early adopters of new technology, somewhat agree to strongly agree.
- 60% currently use a biometric security feature.
- 50% said they would consider using a single biometric feature to replace passwords.

The data shows that age is not a crucial factor in acceptance, as results for all age groups are similar without wide variation. The results for both groups are roughly the same for both male and female, so gender does not appear to be a factor. Acceptance does show a higher rate for all groups based on education level and income.

V. CONCLUSIONS

A diverse range of demographics were represented in the biometric security acceptance survey. There was a roughly even split between male and female respondents indicating a balanced sample based on gender. A wide range of those taking the survey were of different ages, occupations, and income levels and had a high level of past exposure to biometric security applications. Based on sample size methodology, a confidence rate of at least 95% for the survey was achieved with the 410 people that responded.

Of those who took the survey, most manage numerous accounts and are reusing less secure usernames and passwords, which they acknowledge as a security risk. With widespread acceptance of biometric security technology, the need to manage a large and ever-growing number of accounts with unique and strong passwords could be virtually eliminated.

Those who have accepted biometric technology are pleased with the relative ease of use, convenience, and increased security offered. Raising awareness and overcoming objections such as privacy and data safety issues will help promote wider acceptance of the technology.

Cost is also a factor, as most respondents indicated that they would be willing to pay little or nothing for a proven reliable and secure biometric security application. This suggests that an increased burden will lie with businesses, companies, and developers to absorb additional biometric security costs to facilitate wider acceptance among users.

The majority of respondents in all age groups described themselves as relatively early adopters of new technology. Most of them also had an education level of a two- to four-year college degree or above and had income levels above or well above median level. The data supports the hypothesis that more educated people at higher income levels are more willing to accept biometric security; however, it also suggests that age is not a defining factor. Future research may reveal ways to increase biometric security acceptance among less educated and lower income demographics. This research may aid in achieving more widespread acceptance of secure, convenient, and easy to use biometric security applications in place of less safe and harder to manage "knowledge-based" security methods such as passwords and usernames.

VI. FUTURE WORK

As a follow up to this survey, hands on in person testing and feedback from actual users of a biometric security device such as a palm vein or fingerprint scanner would be beneficial.
Obtaining information from a wider geographic area to obtain data from a broader demographic range of respondents will help to validate the data and improve the confidence rate. This could possibly be done by coordinating data gathering with other schools and organizations. Exposure to a multi factor authentication method to include scanning of many biometric factors at once such as Google Abacus will also provide feedback on acceptance of cutting edge biometric security. A comparison of answers prior to and after actual use of the device should provide insight as to the user's eventual comfort level with biometrics.

One of the main objections to acceptance in this survey is concern about a biometric security profile being compromised. Future study of methods to address this problem can help to address this objection. The solution might be something as simple as putting a time stamp or security certificate on a biometric profile and invalidating or resetting it if it has been compromised. Multi factor authentication may also provide a stronger defense against a data compromise.

Provisions for special needs groups also need to be addressed. Though biometric security has advantages, it is probably not wise to attempt to do away with usernames and passwords altogether. They would still be useful to address the needs of these groups and to act as a second line of defense behind biometrics for other users.

Companies will need to assure potential users that their data is safe, using methods such as high-level encryption and hardened data centers, and aggressively promote these features. An increase in testing and input from end users in the design phase may also help to raise awareness and make the transition from knowledge-based to biometric security easier. This is especially important in how it relates to making the application easy to use, learn, and rely on. In an article aimed at banks looking to use biometrics as a form of mobile security, Hung [9] suggests that accuracy, safety, and ease of use are primary factors for financial institutions in choosing a mobile biometric security application. She also stresses that the application should work for more than 90% of their mobile customers and be promotable for wide acceptance.

Apple has embraced biometric security on the iPhone and may serve as a model for other companies and applications. The Touch ID on the iPhone is a fingerprint scanning authentication device first introduced in 2013. Theft of smartphones is a major problem especially in major cities, where it can account for up to 40% of reported crime. [20] The widespread adoption of Touch ID has served as a deterrent to the theft of iPhones, since the fingerprint scan makes it so hard to access. “Given Apple’s influence, the company’s adoption of the fingerprint-scanner technology could increase the use of biometrics in identity verification and accelerate the demise of the password, which many feel has become outdated” [20].

Major online companies such as Amazon and Facebook need to strike a balance between making their sites easy to sign up with, using lax minimum requirements such as six character passwords, versus requiring more security to protect their users. A biometric security option may be the solution.

VII. APPENDIX A

The following is a transcription of the biometric security acceptance survey used for the research in this paper, along with the percentage of respondents selecting each answer option. There were 410 respondents. Question 1 is a validation and disclaimer question discussed in the Methodology section. Questions 2 through 7 are standard demographics-gathering questions regarding gender, age, education levels, occupation and income level.

8. What types of biometric security technology have you used in the past? (Choose all that apply)

Fingerprint scan	75%
Eye (retina or iris) recognition	20%
Voice or speaker recognition	33%
Behavioral, gait recognition	3%
Other	2%
None of these	20%

9. Do you own a smartphone, tablet or another device that includes a security feature such as fingerprint scan?

Yes	76%
No	24%

10. Please check all that apply to your personal use of the biometric security feature on your device.

I use the biometric security feature.	76%
I do not use the biometric security feature	24%
Tried it, doesn’t seem to work well	9%
Other	0.7%

11. Please rank yourself based on the following statement: “I am an early adopter of new technology.”

Strongly Agree	19%
Agree	28%
Somewhat agree	27%
Neither agree nor disagree	8%
Somewhat disagree	8%
Disagree	6%
Strongly disagree	4%

12. When creating new passwords, would you consider yourself most likely to:

Create strong passwords with long phrases	
Use letters, numbers and special characters	63%
Use what is fastest and easiest to remember	37%

13. When creating new passwords, how often do you use one that is unique?

I always use a separate unique password	19%
Most of my accounts use a unique password	29%
Only a few of my accounts use a unique password	44%
Never, I always use the same password	8%

14. How many total username/password accounts do you estimate that you currently use? Please include all personal, business and work related.

1-10	40%
11-20	28%
21-30	14%
More than 30	18%

15. If you live in the U.S. select Strongly Agree

Do Not Agree	6%
Somewhat Agree	4%
Strongly Agree	90%

16. Would you consider using a single biometric security application to replace the need for you to use multiple usernames, passwords, and PIN (Personal Identification Numbers)?

Yes	50%
Maybe	38%
No	12%

17. Which of the following would you consider a positive factor to using a single biometric application to replace usernames, passwords, and PIN (Personal Identification Numbers)? (Choose all that apply)

Increased ease of use	65%
Increased security	64%
Increased convenience	63%
Other	0.31%
None of these	0.31%

18. Which of the following would you consider a barrier to using a single biometric application to replace usernames, passwords, and PIN (Personal Identification Numbers)? (Choose all that apply)

Safety of my personal biometric data	45%

Concern that the biometric application could be hacked or stolen	55%
Cost	22%
Risk of having personal authentication data all in one place	55%
Other	6%
None of these	3%

19. How much would you be you willing to pay per month for a proven biometric security application to avoid using usernames, passwords and PIN numbers for your accounts?

Nothing	49%
$1-$10	40%
$11-$25	9%
More than $25	3%

20. Please rank yourself based on the following statement: "I am not an early adopter of new technology."

Strongly Agree	6%
Agree	12%
Somewhat agree	14%
Neither agree nor disagree	7%
Somewhat disagree	17%
Disagree	25%
Strongly disagree	19%

21. Do you consider biometric security scans to be intrusive?

Yes	18%
No	52%
Maybe	30%

22. What causes you to feel that biometric scans are intrusive? (Check all that apply)

I don't want to share my personally identifying characteristics	61%
Social, cultural or religious reasons	11%
Aversion to physical contact with the device, especially if shared/public	28%
Being tracked to update or maintain a biometric profile	52%
None of these	7%
Other	4%

References

[1] *Adweek*, "Here's how many people are on Facebook, Instagram, Twitter and Other Big Social Networks," April 4 2016, www.adweek.com/socialtimes/heres-how-many-people-are-on-facebook-instagram-twitter-other-big-social-networks/637205, accessed November 2016.

[2] Dashlane, Inc., "[PRESS RELEASE] Dashlane's Password Security Roundup: Most popular websites leave consumers exposed after Heartbleed," March 2014, https://blog.dashlane.com/press-release-dashlanes-password-security-roundup-popular-websites-leave-consumers-exposed-heartbleed/, accessed December 2016.

[3] F. D. Davis, "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results," Doctoral Dissertation, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, 1986.

[4] Department of Numbers, "U.S. Household Income," http://www.departmentofnumbers.com/income/us/#family, accessed November 2016.

[5] Mohamad El-Abed, et al., "A study of users' acceptance and satisfaction of biometric systems," 2010 IEEE International Carnahan Conference on Security Technology (ICCST), IEEE, 2010.

[6] S. Furnell and K.L. Thomson, "Recognising and Addressing 'Security Fatigue,'" *Computer Fraud and Security*, Nov. 2009, pp. 7–11.

[7] Gartner, Inc., "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020," Gartner Press Release, www.gartner.com/newsroom/id/2636073, accessed October 2016.

[8] April Glaser, "Biometrics Are Coming, Along With Serious Security Concerns," *Wired*, March 9, 2016, www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/, accessed October 2016.

[9] Tinna Hung, "5 Considerations When Evaluating Biometrics for Mobile Banking," Eyeverify.com blog, 10/31/16, www.eyeverify.com/blog/5-considerations-when-evaluating-biometrics-for-mobile-banking?utm_content=42489607&utm_medium=social&utm_source=linkedin, accessed November 2016.

[10] Hee Cheol Kim, "A Disciplinary Framework to Study User Acceptance of Innovative Technologies," 2014 International Symposium on Computer, Consumer and Control (IS3C), IEEE, 2014.

[11] Mark Alexander Kowtko, "Biometric Authentication for Older Adults," 2014 IEEE Long Island Systems, Applications and Technology Conference (LISAT), IEEE, 2014.

[12] Kat Krol, Simon Parkin, and M. Angela Sasse, "I don't like putting my face on the Internet!: An acceptance study of face biometrics as a CAPTCHA replacement," 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), IEEE, 2016.

[13] Alina Krupp, Christian Rathgeb, and Christoph Busch, "Social acceptance of biometric technologies in Germany: A survey," 2013 International Conference of the Biometrics Special Interest Group (BIOSIG), IEEE, 2013.

[14] A. Mihai, "Google's Project Abacus aims to replace password based authentication systems," phonearena.com, May 29, 2015, www.phonearena.com/news/Googles-Project-Abacus-aims-to-replace-password-based-authentication-systems_id69874, accessed October 2016.

[15] Ian Morris, "Google's Chrome Web Browser is Killing Your Laptop Battery," Forbes.com, July 14, 2014, www.forbes.com/sites/ianmorris/2014/07/14/googles-chrome-web-browser-is-killing-your-laptop-battery/#7e4671aa2bec, accessed October 2016.

[16] B. Oto, "When Thinking Is Hard: Managing Decision Fatigue," *EMS World*, vol. 41, no. 5, 2012, pp. 46–50.

[17] Pew Research Center, "America's Shrinking Middle Class: A Close Look at Changes Within Metropolitan Areas," May 9, 2016, www.pewsocialtrends.org/2016/05/11/americas-shrinking-middle-class-a-close-look-at-changes-within-metropolitan-areas/st_2016-05-12_middle-class-geo-03/, accessed November 2016.

[18] Abdullah Rashed, Henrique Santos, and Arwa Al-Eryani, "Biometrics acceptance in Arab culture: An exploratory study," 2013 International Conference on Computer Applications Technology (ICCAT), IEEE, 2013.

[19] Joseph Romanowski, Kirsanov Charles, Patricia Jasso, Shreyansh Shah, and Hugh W. Eng, "A Biometric Security Acceptability and Ease-of-Use Study on a Palm Vein Scanner," Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 6, 2016.

[20] Gerry Smith, "iPhone Fingerprint Scanner Comes with a Catch," Huffington Post, September 11, 2013, http://www.huffingtonpost.com/2013/09/10/iphone-fingerprint-scanner_n_3900529.html, accessed November 2016.

[21] Scott Smith, "Determining Sample Size," Qualtrics blog, April 8, 2013, www.qualtrics.com/blog/determining-sample-size/, accessed October 2016.

[22] Scott Smith, "4 Ways to Ensure Valid Responses for Your Online Survey," Qualtrics blog, April 22, 2013, www.qualtrics.com/blog/online-survey-valid-responses/, accessed October 2016

[23] Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman, "Security Fatigue," *IT Professional*, Sept.-Oct. 2016, pp. 26-32.

[24] Darlene Storm, "Worst, most common passwords for the last 5 years," Computerworld, January, 2016, www.computerworld.com/article/3024404/security/worst-most-common-passwords-for-the-last-5-years.html, accessed October 2016.