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

Biometric Authentication: Solution for All?

Eiman Ahmed, Brandon DeLuca, Emily Hirowski, Connor Magee, Ivan Tang, and Jean F. Coppola
Seidenberg School of CSIS, Pace University, New York, New York

***Abstract*—As technology continues to grow and advance at a rapid rate, most producers and companies are neglecting a rather large demographic: the elderly. The elderly, who are accustomed to more traditional means of communication utilizing pencil and paper, are having difficulty keeping in stride at the same rate as technology is pacing itself in the modern era. Cyber security, one of the most vital aspects of technology, is an area in cyberspace where senior citizens are struggling to adjust. Although they understand the necessity of having passwords to keep their private information secure, they often grow frustrated with remembering their passwords, which may vary from website to website and are often strenuous to remember due to regulatory password procedures. The objective of this project is to investigate how this issue can be tackled in a simple manner using biometrics. Biometrics is the most secure form of authentication to date, regardless of one's age. In this study, older adults from geriatric centers are assessed with questions in regards to how they currently manage the various passwords they create for their accounts, how they feel about their current management methods, and methods they feel their experience can be enhanced more than it already is. In addition, different biometric technologies, e.g., retinal, fingerprint, facial recognition, etc., is compared to one another and a proposed solution of the framework that would be free of cost to older adults.**

Keywords-authentication; older adult; password; privacy; recognition; security; senior citizen

I. Background

As technology advances continue to be made and new generations continue to utilize new phones, tablets and games, it has become apparent that a generation has been left behind. In a rush to accommodate younger children with advanced technology, companies have left behind the elderly, a generation which has had trouble associating with even the most basic forms of technology. Above all issues and fields opf study, cyber security has become the most prevalent computer science topic in modern day; with hacking tools and knowledge now widely available on the internet, there is now a greater chance than ever that one's information can be stolen, even if one is not fooled into "handing" this information over.

Seniors are often discouraged from learning to use new technologies because of their physical limitations, as well as being tasked to learn how to use the devices. Phones and tablets, for example, are relatively small and are thus difficult to read from for seniors with visual impairments; they are not as popular with older adults as they are with younger generations. Memory problems also create issues with remembering passwords; this may force older adults to write things down to keep track, which is a huge security flaw. The inevitability of being hacked means that cyber security seeks to prevent hacking attempts, not completely rule it out; the proper precautions need to be taken.

Most recently, however, Smith has found that this trend in skepticism from older adults towards technology is shifting as although new technologies are difficult for them to keep up with, the benefits they have toward everyday life exceed those negative aspects [1]. According to Pew Research Center [1], 79% of older adults who use the Internet agree with the statement that "people without internet access are at a real disadvantage because of all the information they might be missing," while 94% agree with the statement that "the Internet makes it much easier to find information today than in the past."

One of the greatest advantages and key reasons as to why many older adults are turning toward the Internet and technology now is social media. In a recent study conducted by researchers Michael Braun and Lyn Van Swol Ph.D. from the University of Wisconsin, it was found that around 44% of adults aged 60-90 said they periodically use social networking as it is user friendly, useful, and popular amongst their communication circles [4]. Seniors often do not get to experience as many social interactions as other people do due to either being homebound or unable to travel frequently. Social media is useful to them in this scenario as it allows them to still feel engaged with the outside world, while remaining in the comfort of their own homes.

As technology continues to integrate itself into the everyday lives of people and future generations, seniors must begin to feel comfortable with these new technologies for a better means of living. Most seniors are already beginning to take the first step towards doing so, however, there still needs to be many more advancements made in bridging the gap between the younger generation who is fluent in technology and older adults who are afraid of it or discouraged by it. Perhaps most importantly, older adults must feel must have a shift in paradigm so that they themselves are more inclined to learn about these new technologies as well.

II. Introduction

Cyber security is the collection of advances; procedures and practices intended to secure systems, PCs, programs and data from attack, harm or unapproved access. In technological context, security incorporates both cyber security and physical security. A standout amongst the trickiest components of cyber security is the rapidly and continually developing nature of security dangers. The conventional approach has been to concentrate most assets on the most vital framework segments and ensure against the greatest known dangers, which required abandoning some less imperative framework segments undefended and some less dangerous risks not protected against. To manage the present environment, advisory organizations are advancing a more proactive and versatile approach. The National Institute of Standards and Technology (NIST), for instance, as of late issued redesigned rules in its risk evaluation system that prescribed a move toward constant observing and continuous assessments.

Passwords are utilized on websites throughout the Internet. Passwords ensure users' personalities on sites, discussion boards, emails and that's only the tip of the iceberg. Numerous family PCs with different accounts utilize passwords. They are additionally utilized for bank exchanges and making secure purchases. With the greater part of this touchy information in question, making great passwords is essential to avert data fraud. Passwords are the primary barrier against PC hackers. Programmers normally attempt to break into a PC or secure record by speculating passwords. Computerized projects can likewise be utilized to more than once figure passwords from a database of regular words or other data. A solid secret password is imperative to buy time, counteract assaults by less dedicated hackers, and send up warnings that can catch such fraudsters in the act.

Most passwords are case sensitive. This implies that capitalization counts: "password123" is unique in relation to "Password123" neither of which is a great password to use. Capitalizing the first letter or any letter in the password, using keyboard symbols such as ampersand, pound, percent, and creating passwords that are at least eight characters long are amongst some of the more common requirements for passwords these days. However the majority of individuals utilize exceptionally frail passwords. In addition, the majority of people also tend to reuse their passwords on various sites. Password reuse is a major issue in view of the numerous password leaks that happen every year, even on expansive sites. At the point when your password releases, malevolent people have an email address, username, and password combination they can attempt on different sites. On the off chance that you utilize the same login data all around, a hole at one site could give individuals access to every one of your records. On the off chance that somebody accesses your email account along these lines, they could utilize password reset connections to get to different sites, similar to your web based bank accounts or PayPal account.

Password managers are a solution to this type of problem, as they are able to store login data for every one of the sites people utilize and help them sign into them consequently. They encode user passwords into a database with a master password and use this password as the single password that the user must remember. Biometrics is another solution to this problem as it rids the user of having to remember any password at all and simply uses their physical features such as their face, in the case of facial recognition, or their fingers, in the case of fingerprint scanning, as their password.

This study focuses on senior citizens, who are reluctant towards using new technologies and often stray away from technology due to either finding it difficult to use or strenuous in some way, feel about using biometrics as a means of storing their user information and passwords as opposed to the more traditional means of storing their user information and passwords in either their memory or on some sort of paper or notebook. From this study, derive solid conclusions as to how older adults view technology, Cyber security, and biometrics as a whole.

III. Data And Methods

For this research, twenty-five older adults were surveyed ranging from ages fifty to ninety from geriatric centers across Manhattan. For the purposes of data collection, older adults were observed and notes were made on how they currently manage their passwords, before introducing them to biometric authentication as a new means of authentication. The older adults were then asked to try biometric management hardware and software, such as USB fingerprint scanners, eye scanners, and Intel's TrueKey software, and then to make conclusions and answer questions.

IV. Results And Analysis

To start the analysis off, it was necessary to see if there was any discourse amongst older adults themselves and how often they currently tend to use technology. Of the twenty-five older adults surveyed, it was found that those between the ages of 50-59 use technology the most out of all the other age groups, with around 77% of older adults in this division saying that they either "somewhat" or "strongly" agree that they use technology often (See Figure 3.1), while 100% of older adults between the ages of 70-89 responded by saying the converse, that they "somewhat" disagree with this statement (See Figure 3.2). This data indicates some form of a technology gap between even older adults themselves. Although those between the ages of 60-69 seemed to appear more neutral on the matter, the shift from most interviewees using technology often to rarely using technology at all may be evidence that as people age, they are less inclined to using technology as a whole.

Figure 3.1

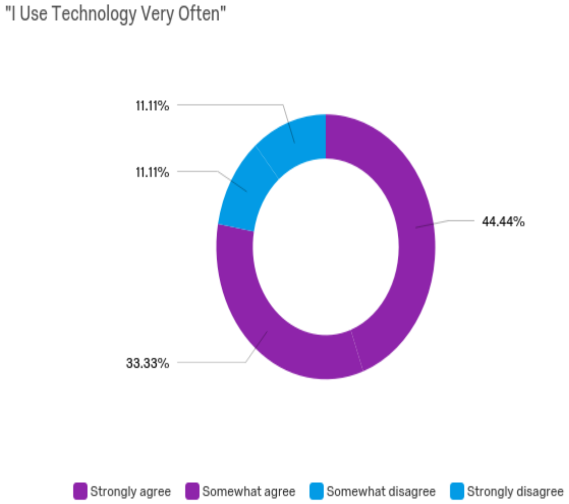
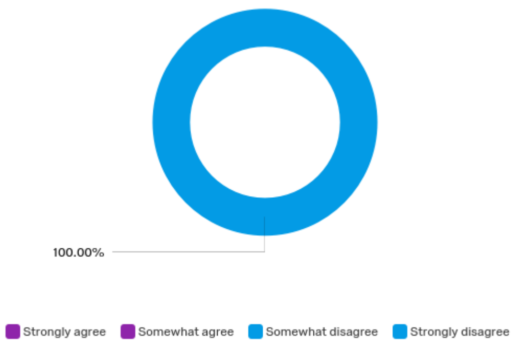


Figure 3.2

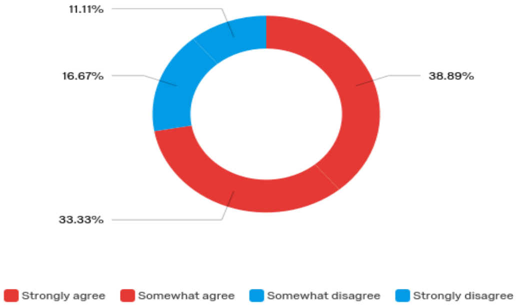
"I Use Technology Very Often"



In order to better understand the nature of customary passwords with older adults, especially in the nature of how lengthy and complicated they may sometimes be required to set as, the older adults were asked how long they felt typing their passwords took them. This is not subject to, but includes finding their passwords, inputting their passwords in, and of course any mismatch of passwords, in which they would have to re-enter their passwords into the system. From this, analysis show that around 72.22% of older adults felt that typing in passwords took a rather long time, showing that current means of storing and creating passwords is not time efficient and thus calls for change in paradigm (See Figure 3.3).

Figure 3.3

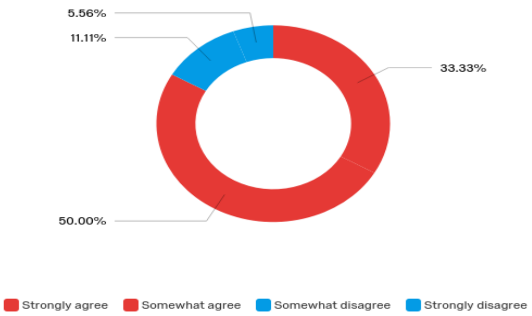
Passwords Take a Long Time to Type



Because the study revolves around the current limitations in standard password storage and understanding whether biometrics may be a better solution to this issue, older adults were asked whether they found keyboards difficult to use. Of the surveyed seniors, 83.33% felt that keyboards were difficult to use (See Figure 3.4). The issue thus expands, not only from the majority of older adults finding it inefficient to type in traditional passwords, but also to use keyboards in order to type these passwords. Given this data, it can be concluded that perhaps because such an overwhelming amount of older adults feel that keyboards are difficult to use, they take longer to type out their passwords; Also indicating yet again a drive to create a new form of inputting passwords onto systems.

Figure 3.4

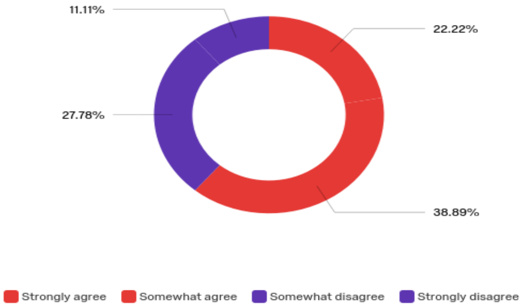
Keyboards Are Difficult to Use



Given the past analyses, it was thus rather surprising that when asked whether they found biometric options to provide a better experience than traditional password options, although the majority of older adults said that they felt the biometrics option provided a better experience for them than the former, only 61.11% of older adults felt this way, even though 83.33% of these older adults felt that old means of typing out passwords was more difficult (See Figure 3.5). This study doesn’t go into the specifics, however, this could mean that either they felt more indifferent towards biometric scanners or they found them almost equally as challenging as older methods of storing passwords such as through keyboards.

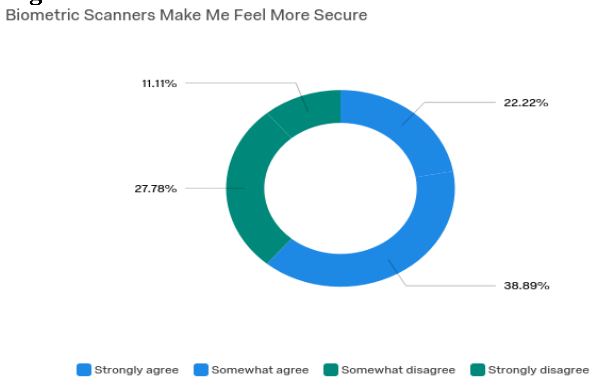
Figure 3.5

Biometric Scanner Experience



Rather similar results were shown when these seniors were asked how secure they felt using biometric scanning options as opposed to other options. Around 61.11% of older adults said that they felt more secure using biometric scanners, thus suggesting a preference towards biometric options when it matters relating to security (See Figure 3.6).

Figure 3.6



To better understand the importance of security and passwords in relation to older adults using technology, seniors were surveyed on whether or not remembering or typing passwords ever drove them away from technology. Around 38.89% responded by saying that they felt as if their was some sort of correspondence between them turning away from some forms of technology due to having to remembering and typing out their passwords (See Figure 3.7). The majority of adults who shy away from technology most likely do so for some other reason unrelated to this issue. Passwords do not seem to be most seniors' main concern when it comes to using technology, that biometrics and involving seniors with biometrics for the sole purpose of drawing them closer towards technology is not the ideal solution to this specific problem. Nonetheless, around 88.89% still said that would feel more inclined to use security features if they were made more accessible to them, either in the form of biometrics or otherwise which proves that current methods of security are not as accessible or ideal as they can be (See Figure 3.8).

Figure 3.7

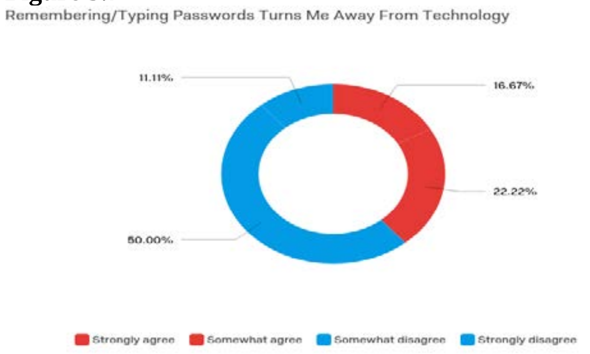
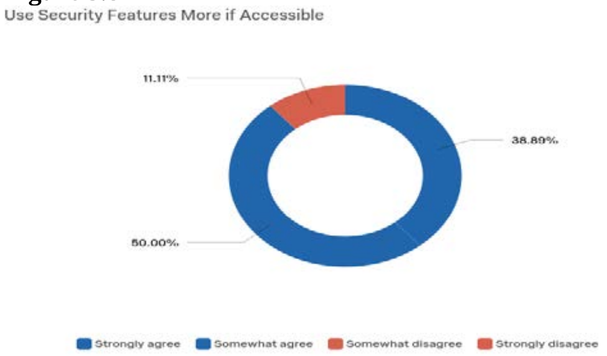
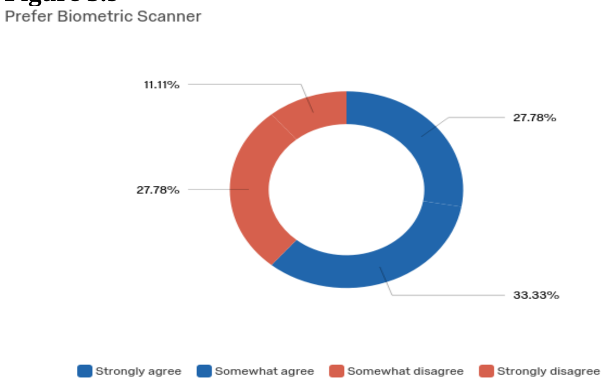


Figure 3.8



Ultimately, however, through the survey around 61.11% of older adults said that they preferred biometric scanning options to the traditional keyboard in terms of creating and storing their passwords for them (See Figure 3.9).

Figure 3.9



CONCLUSION

Through this study, the conclusion is although security isn't the primary concern of older adults when it comes to technology; they still find typical methods of storing and loading passwords to be rather exhausting and troublesome. They would be more inclined to using security features if they were made to be more accessible and even though it is not by much, they prefer biometric scanning to keyboard entering options, perhaps because the majority of them find keyboards hard to use and typing in passwords to be a hassle. Finally, typing in and remembering passwords is not a major factor in most of them using technology more often than they currently do or do not. Thus, although biometrics is a useful tool and most older adults prefer it over their other options, it needs to be more improved and their needs to be more research conducted as to why only a select few seemed to prefer biometric options over keyboard options, when so many found keyboards to be difficult to use and current means of storing passwords to be so burdening.

FUTURE WORK

In the future, this research will be expanded by testing out a variety of biometric systems and comparing and contrasting the bunch to one another to see whether any biometric systems or platforms perform better than others with older adults. Additionally, more data will be collected with a greater volume of people and in different locations, not the greater New York City area.

ACKNOWLEDGEMENTS

Thank you to Professor Jean Coppola, and all of the seniors who volunteered to take this survey for this study to aid in conducting the research required for this paper and providing the foundation for the development of the work and analysis.

REFERENCES

[1] A. Smith, "Attitudes, Impacts, and Barriers to Adoption." *Pew Research Center: Internet, Science & Tech*., Pew Research Center, April 3, 2014.

[2] S. Brink, "Digital Divide or Digital Dividend? Ensuring Benefits to Seniors From Information Technology." *Government of Canada Publications*. Minister of Public Works and Government Services Canada 2001, Sept. 2001.

[3] A. Kamiel, "A Hot Trend: The Internet, Social Media & The Elderly." *The Huffington Post*. TheHuffingtonPost.com, Mar. 7, 2016.

[4] Braun, Michael, and Lyn Van Swol. "Obstacles to Social Networking Website Use among Older Adults." Obstacles to Social Networking Website Use among Older Adults. University of Wisconsin, n.d. Web. 5 Jan.2017.

Eiman Ahmed is a third year computer science major at Pace University in the NYC campus. As both a Pforzheimer Honors and Seidenberg student, she is looking to pursue a PHD in AI and machine learning after she completes her undergraduate studies. In the past two years, she has interned as a software developer at Microsoft and as a data science student researcher at Microsoft Research. She has also presented at multiple conferences including the conference on digital experimentation at MIT, the Northeast regional honors college conference, and the IEEE conference at MIT where she received the title of honorable mention for her poster presentation on the research she completed in accordance with Microsoft Research. This past year, she has founded an organization to empower other women in the computing discipline called the Pace Women in Tech: Lean In Circle. During her final few semesters at Pace, she hopes to see it continue to grow and prosper and serve as a safe space where students can develop relationships within the industry and spread their resources to one another.

Emily Hirowski is a Sophomore Biology major at Pace University. She is currently involved student-faculty research in the Biology Department and is studying the effects of mutations in voltage-gated calcium ion channels found in neurological disorders. In the laboratory, Emily has obtained training in electrophysicology, primer design, DNA extraction and RNA exdtraction. She is also a Biologypeer leader in the fall Semsters at Pace. She guide students taking General Biology through weekly asignments aimed at helping them understand basic biology material taught in lecturs. Emily has alosobtaind CPR certification from the American Red Cross Greater New York location and hopes she can use this training to help people in possible life-threatening emergencies.

Brandon DeLuca is a second year Computer Science student at Pace University NYC, and a member of the Pforzheimer Honors College. He is extremely interested in the growing field of Cybersecurity, and is currently minoring in Information Assurance studying for CompTIA's Security+ exam; in a world where more and more battles are being fought online, Cybersecurity has the ability to change the world. Biometrics is known in

Cybersecurity as the most secure form of authentication, so it is necessary that we analyze its effect on the elderly. Brandon is also a co-founder of the Cybersecurity Club at Pace University, where he is the Vice President. He currently works in the computer lab on campus as an IT Specialist, assisting students and faculty with problems they may have on their personal/school-owned machines. He has previously worked as an IT Help Desk/Assistant System Administrator at the Union for Reformed Judaism, a Field Technician for the NYC Department of Education, and an IT for all four years while attending Fort Hamilton High School. He was also a finalist of Pace's Twelth Annual Pitch Contest, and took Second Place in Functionality at Westchester's Second Annual App Bowl for his T13 Keyboard, which is available on Google Play.

Ivan Tang is a full time freshman Computer Science major with a minor in Information Security, at the Seidenberg School of Computer Science and Information Systems. He has an expected graduation in May 2019. He currently lives in Brooklyn, New York. He has grown up with computers and is always constantly attempting to learn more about computers and technology. In high school, Ivan joined the tech squad for his duration at Fort Hamilton. Alongside with Dr. Coppola, he hopes to make technology more efficient for the elderly. Technology is moving very fast and is very innovative and doesn't wait up for the elderly. With his classmates, Ivan was a finalist in the Pace Pitch Contest and placed second place for functionality in the Westchester Mobile App Development Bowl. In the future, he hopes to use his knowledge in computer science to aid people and make their lives simpler.

Connor Magee is a full time undergraduate student at Pace University of the New York City Campus. He is a student within the Seidenberg School of Computer Science and Information Systems and is expecting to graduate in the spring of 2019 with a B.A. in Computer Science. Connor is currently working for the New York Police Department and the Applied Data and Networking Science Lab at Pace University. At the New York Police Department he works on the Information Security team, working to help prevent the network from attackers and malicious users. In the Applied Data and Networking Science Lab, Connor acts as the TA, helping students learn about the field of cybersecurity. After graduation, Connor plans to become a penetration tester or cybersecurity consultant. His studies at Pace University has a focus on cybersecurity, learning about different fields from network security to system exploitation. Throughout his work at these jobs, Connor has gained much experience, theoretical and hands on, dealing with routers, switches, mobile devices, laptops, desktops, and servers. He is also the President and Founder of the CyberSecurity Club at Pace University. At this club, students come in with an interest in the field of cybersecurity, and he as well as other members of the club help guide prospective students.

Jean F. Coppola has been an IEEE member for over 20 years. Dr. Coppola is a tenured faculty member in the Department of Information Technology, Seidenberg School of Computer Science and Information Systems, Pleasantville, New York, where she has employed with Pace University since 1986.

Dr. Coppola received her B.S. in Computer Science from Hofstra University in 1986. She received both her M.S. in Computer Science in 1990 and M.S. in Telecommunications in 1992 from Pace University. She received her Ph.D. in Computing Technology in Education from Nova Southeastern University in 2003. Dr. Coppola has authored numerous articles and papers, and has presented in many conferences on topics including gerontechnology, service-learning, assistive technology, and telehealth

Dr. Coppola is an award winning educator, author, and speaker being honored with the Jefferson Award for Public Service, Computerworld Laureate Award for visionary applications of information technology to promote positive social, economic and educational change, Wilson Foundation Faculty Fellow, Women Builders of Communities and Dreams Award, Westchester Women in Technology, and the EMG Health Communications, honored for outstanding community commitment and outreach to elderly. She is advisor to many award winning student academic teams that develop assistive devices and mobile apps targeted to help dementia / Alzheimer patients, caregivers, as well as the disabled and elderly. Current research focuses on gerontechnology, concentrating on intergenerational assistive telehealth Remote Patient Monitoring to improve older adult quality of life, increase cognitive functioning, and provide positive student attitude change towards elderly.