A Study of Smartphone and Laptop Security Acceptability and Ease-of-Use

Recognition Technologies, Inc., U.S.A.
Technical Report: RTI-20150501-01

Jimmy Leon, George Chacko, Hugh Eng, Daniel Weise, and **Emmanuel Ruiz**
Seidenberg School of CSIS, Pace University, White Plains, New York

Homayoon Beigi
Recognition Technologies, Inc., White Plains, New York
beigi@recotechnologies.com

Abstract - As technology evolves, security plays a crucial role in physical security such as a door or technical security for a system, application or website. The standard username and passwords in today's society are inconvenient, insecure and just not adequate. They are considered ineffective to modern world hackers. As more and more sensitive data is exposed, the need for a more robust system that fuses multiple modes of authentication is needed. The benefit of biometrics is that it presents us with information that is accessible and unique to each individual. A high level of accuracy can be obtained by using the multimodal biometric, multifactor authentication system of Recognition Technolopgies, Inc. (RecoMadeEasy® Access Control). The study performed shows that a biometric authentication system is largely accepted, easy to use and more secure then the engrained username and password.

Index Terms—Biometrics, Face Recognition, Voice Recognition, Speaker Verification, Multifactor Authentication

ACKNOWLEDGEMENTS

It is with immense gratitude that Team 2 of Spring 2015 acknowledge Dr. Beigi from Recognition Technologies, Inc. for allowing us to use his RecoMadeEasy® biometric systems. Spring 2014 Team 2 for the foundation of the project and recommendations. Dr. Tappert for his guidance on the project and last DPS candidate Hugh Eng for always following up with us on the status and advising necessary approaches with the project. Without their support guidance and persistent help, this technical research would have not been possible.

I. Introduction

Some biometric systems are more acceptable by users than others - for example, most users don't like to have their retinas scanned because the equipment is intrusive, the user having to place his/her face into a device for the scan. Biometric systems also vary in their ease-of-use. This project will conduct usability studies to evaluate the acceptability and the ease-of-use of a biometric system that uses two or more modalities fused together for user authentication. Recognition Technologies, Inc. allowed us to use its proprietary facial, speaker[2] (voice) and speech recognition to conduct this study. [1]

Biometrics uses human characteristics to interface with a system and provide authorization and access to a specific area or program; this can be both hardware and software based. Biometric identifiers can be physical or interactive. We will test the use of facial, speaker (voice) and speech recognition and discuss other modalities used in biometric authentication such as fingerprint scans, finger, hand and ear geometry, and retina or iris recognition.[3] Biometric authentication is the foundation of the future of highly secure identification and personal verification. While a password could be hard to crack, it is only a matter of time before a persistent hacker eventually gains access to a system.[4] With physical biometric identification, it changes the scope of security and authentication. Our study primarily focuses on pin, facial and voice recognition based system, which creates a robust system

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Worn ridges; hand or finger impairment	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectibility	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

Table 1. Comparison of several biometric technologies[1,4]

Published as a technical report of Recognition Technologies, Inc. on May 1, 2015 (DOI: 10.13140/RG.2.1.2103.1848). Contents were also published with the title, "Smartphone/Laptop Security Acceptability/Ease-of-Use Study," in the Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 1st, 2015

for authentication. While the system is not without flaws, our tests found that the technology at hand provides the administrator with ample control to define the parameters by which the user can gain access.

II. METHODOLOGY

A. Study Objectives

Primary - Review the technology behind a multimodal biometric system when applied in a real-world scenario and create video for survey participants to view prior to survey completion.

Secondary - Gather demographic, acceptability, system delay, and ease of use data from target audience.

B. Target Audience

The target audience will come from three collections of users

- Previous semester's study survey responses
- Pace University's students and faculty members
- Social Media

C. Data collection method

Create a survey through a selected survey platform and distribute link via email and social media. The video will be displayed prior to survey completion to give the user the required background knowledge for survey participation. Results are immediate for each participant and are accessible through the survey platform. The dataset can be displayed in multiple forms.

There are many methods in which the collection of survey data through computers can be composed. After some research, we could make the notion that one can classify them based on the type of technology that we are relying upon to distribute the survey we are working with and collecting its data. The best working ways of collecting this are as follows; point of contact, email based, and web based.

1) ***Point-of-contact***

Point of contact involves having the respondent to fill out an e-survey on a computer provided by the researcher, either on-site or in a laboratory setting.[5] Point-of-contact surveys have also been proven to be very productive because it gives us the administrators a sense of complete control and security that the survey is being taken properly and not misused.

This method was actually tested by a member of the team involved in this survey. The member provided an on-site computer where his colleges, friends and students could come and complete the survey. The was indeed proven to be very help has we accomplished to double the amount of survey from the research done in the previous semester.

2) ***E-mail-based survey***

E-mail-based surveys are generally defined as survey instruments that are delivered through electronic mail applications over the Internet or corporate intranets.[6] Electronic mail has been become the most popular form of communicate and authentication in the world. Using this type of communication to conduct surveys is a genius of an idea. We have also use this form as a distribution tool to have our survey in motion of the pubic taking the survey. E-mail is also a best way to distribute a survey in terms of financial matters.

3) ***Web-based***

The last form is electronic survey, and this method is currently receiving the most interest from researchers. This is the type of survey that is usually hosted on a network server or even on an organizations intranet physically, and that will be mainly access through a Web Browser. We would consider this is to be the most "fun" type of survey because it presents the potential to be customizable to whatever the researcher desire. They can be structured to hold animation, voice, video etc. Web-based surveys are often connected directly to a database where all completed survey data is categorized and stored for later examination.

III. SURVEY DESIGN

This project is a continuation of work completed the previous year in which the team created a video of the technology in use and a test survey sent to a small target audience. After review of the content and results, a decision was made to clarify the survey questions and edit/recreate aspects of the original video to show close up footage of the technology's interface. Different gender and age participants were used in the filming. The end result is a video to bring all potential survey respondents into a similar level of understanding.

The video begins with a graphic to gain the respondent's interest in the technology followed by a brief text description of multimodal biometrics and multifactor authentication. Dr. Homayoon Beigi of Recognition Technologies, Inc. then does a short monolog further explaining the use and application of the system. There is also a short monolog to explain the reason for the video, how to access the survey and thanking respondents for their time. The multimodal biometric system is used in this application to open a door. A couple of the user's enrollment process was filmed. The team members and a female child then demonstrated use of the technology going through its normal paces. Multiple scenarios to spoof the system into false authentication were attempted as well. The video attempts to exhibit the ease of use and security of the biometric authentication system so users can make educated responses to the survey. Thresholds were adjusted to show the system could be scaled for greater or less security depending

on the application. Unenrolled, failed authentication attempts, and false positive/negative results were recorded as well.

Phase 2 required creation of the survey. The research suite chosen to host the survey was Qualtrics.com. Concern with survey participation and completion was discussed. Survey research shows that focus on length, format, ease, delivery method and feedback are imperative to a well-designed survey. Proper question wording is important for consistent meaning to respondents. Problems can occur with:

- Lengthy wording - Words are unnecessarily long and complicated.
- Length of question - Question is unnecessarily long.
- Lack of specificity - Question does not specify the desired information.
- Lack of frame of reference - Question does not specify what reference comparisons should be made to.
- Vague language -Words and phrases can have different meanings to respondents.
- Double negatives - Question uses two or more negative phrases.
- Double barreled -Question actually asks two or more questions.
- Using jargon and initials - Phrasing uses professional or academic discipline-specific terms.
- Leading questions - Question uses phrasing meant to bias the response.
- Cultural differences in meaning - Phrases or words have different meanings to different population subgroups. [7]

The survey was kept to 12 short questions with radio button multiple choice answers. The questions were designed to be simple and straightforward. All attempts were made to phrase the questions in order to avoid confusion. No open answers were required. After two demographic questions, the study focuses on questions regarding biometric systems ease of use, acceptability and issues with delay. Qualtrics.com delivers the survey online which would enable participants to complete in the shortest amount of time hopefully increasing the success rate. It is in a scrolling single page format. A link to a web page will be provided with the embedded survey video. The participant can either view the video and then link to the survey or enter the survey directly. The survey can be viewed in appendix of this paper.

After reviewing last year's survey which we found to be pretty useful to guide us in the right directions, we revised question wording and removed a question that was redundant. We added two questions concerning system latency perceived from the actual authentication process and the mechanical delay of the door locks. This could potentially lead to a negative perception of the technology and affect user's decisions.

The importance of this survey is vital for this type of research because it will create an opportunity of development for future and upcoming projects, which contain the same features as this one. Conducting this year's surveys will provides a snapshot of the attitudes and behaviors of the targeted survey population, which will help serve as a baseline to measure and establish a level from where to compare results over time.

IV. RESULTS AND FINDINGS

The video was edited and released under the control of Recognition Technologies, Inc. for copyright purposes. Once approved by the stakeholders, the informational video and survey was launched on April 14th, 2015 and remained open for 7 days. 102 responses were collected. The survey has a 2% drop out rate.

Last semester[8], the survey was initially sent to the primary target at Pace University. The core study team sent the survey to colleagues and friends, Dr. Beigi sent the survey to a combination of academic and professional colleagues. This semester the core study team extended the survey to personal contacts, personal social media and all 11 (eleven) Capstone Teams [9]. A copy of the survey was created for Dr. Beigi to send to his academic and professional colleagues but because of our reduced window from video production and editing, the second survey did not collect any responses. The core study team's goal was to quadruple the pooled respondents from 50 to 200, which we failed to do.

The informational video and survey was launched on April 14th, 2015 and remained open for 7 days. 102 responses were collected. The survey has a 2% drop out rate. All responses were recorded by Qualtrics.com and at the ending of the survey, a spreadsheet was available for download. The spreadsheet provided the responses to all the survey questions, which allowed us to breakdown the results. Below are the breakdown for each question of the survey as it appeared to the target audience.

Question 1 and 2 were simple demographic questions regarding gender and age. The demographics are important in an acceptability and ease-of-use study because certain age groups are more willing to change.

In the survey of 2014, there were significantly more male respondents than female respondents. In our 2015 survey, female respondent increased from 19% to 31% and our male respondents decrease from 81% to 69%. The change in data could have resulted on total amount of pooled respondents in 2015. This time around we were able to double our respondents from 52 in 2014 to 104 in 2015.

As we compare our second survey question with last year's survey, we noticed that both Fig 1 and Fig 1a have similar

baseline of data. In both figures, the 41-55 age group had the most respondent of users. Decreasing responses by age groups were the 25-32, 33-40, 18-24 and ending with the 56+ group with the least respondents.

Answer		Response	%
18-24		14	14%
25-32		24	24%
33-40		24	24%
41-55		30	29%
56+		10	10%
Total		102	100%

Fig. 1. Distribution of age grouping 2015

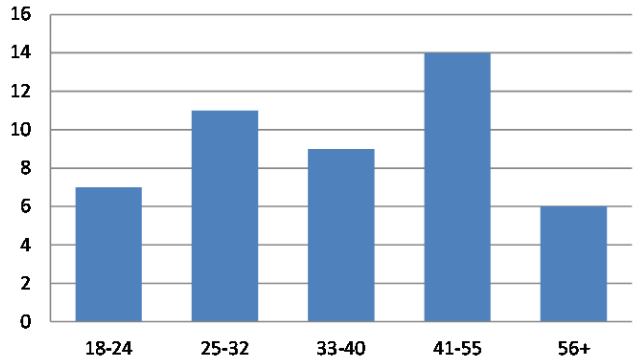

Fig. 1a. Distribution of age grouping 2014

For our third question we decided to modify the 2014 question to "How many unique username and passwords do you think you use on a daily basis?" instead of using the "How many unique username and passwords combinations do you use on a daily basis?". The changes were made to simplify the question for our respondents to understand if they have and use a different username and password for all their types of accounts on a daily basis. Figure 3 below shows that 52% of our survey respondents have up to 5 different, in our case unique, username and passwords. We assume that 53 respondents have 0-5 different username and password that they use for all their accounts they have. In other words if one resondent has 20 accounts and only has one unique username and password, the result is that the respondent uses the same username and password for all 20 accounts. Same scenario goes if one respondent has 20 accounts and has two unique username and password, which can results that each unique username and password having ten accounts. Only 4% stated they have 21 and more unique username and password, which can indicate for each account they have they use and or create a separate username and password for the account.

Figure 3 displays result when respondents were asked how convenient the audio and visual biometric verification system to be. The majority of the survey pool found the technology to be somewhat convenient (47%) followed by extremely convenient (30%) and neutral (17%). Based on the overview and evaluation of this system, we find that biometric verification is viewed to be convenient by the public.

Answer		Response	%
0-5		53	52%
6-10		30	29%
11-15		8	8%
16-20		7	7%
21+		4	4%
Total		102	100%

Fig. 2. Unique login and passwords

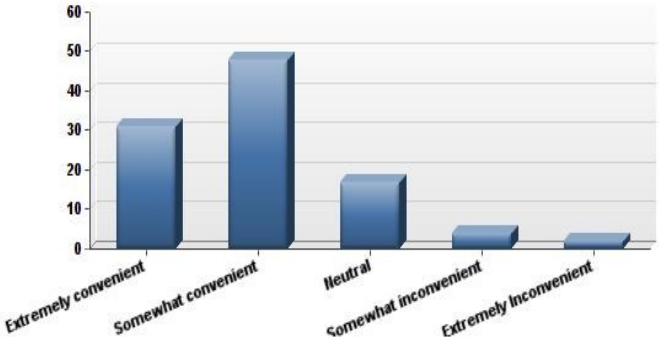

Fig. 3. Perceived convenience

Figure 4 shows how secure the audio and visual biometric verification appeared to the surveyors. The majority found it to be secure with 49% followed by 32% rating it as being very secure. This is often the main topic when it comes to how secure this type of security can be and what it can be trusted with. By means of our audience showing that most of them believe it to be secure, it shows how willing society is in accepting and feeling comfortable with biometric verification.

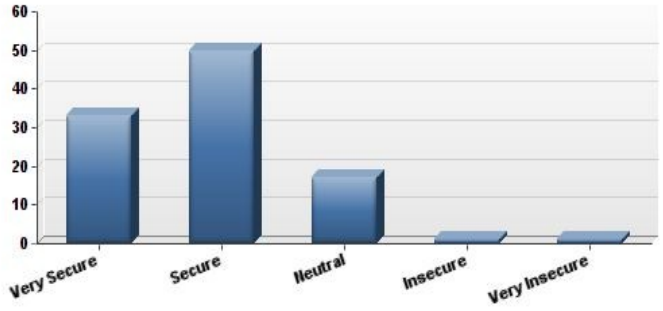

Fig. 4. Perceived security

Figure 5 shows how easy the audio and visual biometric verification appeared to the user watching the video. The survey shows that clearly majority of the surveyors (81%) found the system to be between easy (52%) and very easy (31%). There are many applications and solutions of biometric technology and it has many advantages such as: improved security and effectiveness, reduced fraud and ease of use as clearly depicted in this chart. Biometrics is a part of our future, and they stand to improve the ease-of-use while bolstering corporate security and enhancing user privacy.

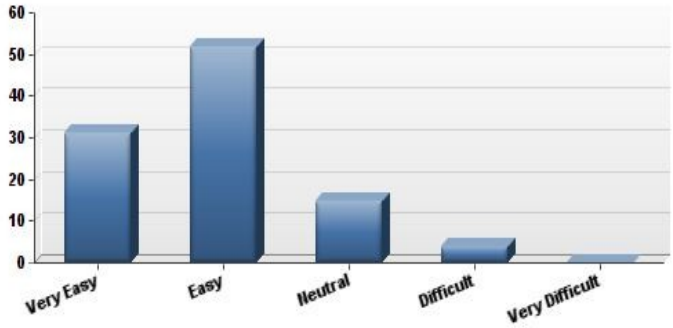

Fig. 5. Perceived ease-of-use

Figure 6 displays results when users were questioned on the perceived delay time between the biometric verification and the system granting access to the user. There was concern after the previous semester's work that the system had a delay that would possibly cause users to reject the biometric system. The surveyors seem to be split on this as 56% did not feel there was a significant delay in the time, where the system was being a hindrance. However, 44% of the surveyors did find that there was a significant lag between the two sequences. During testing, it was determined that access was either granted or denied rather quickly but the actual perceived delay was caused by the mechanical door lock solenoid.

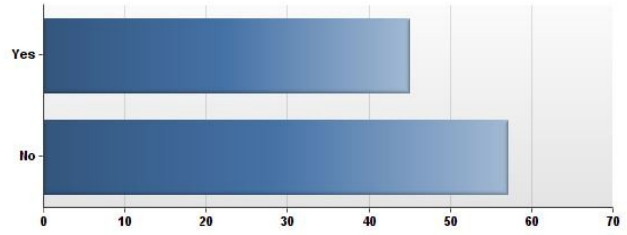

Fig. 6. Perceived delay

The question of delay led to a question of how much delay would be acceptable for a user to still adopt a biometric system. Figure 7 shows surveyors would be ok having a delayed response for higher security. Most of the surveyors preferred lesser authentication times, however, for sensitive information such as medical records, border crossing and banking information some surveyors did prefer a slower and more robust authentication system.

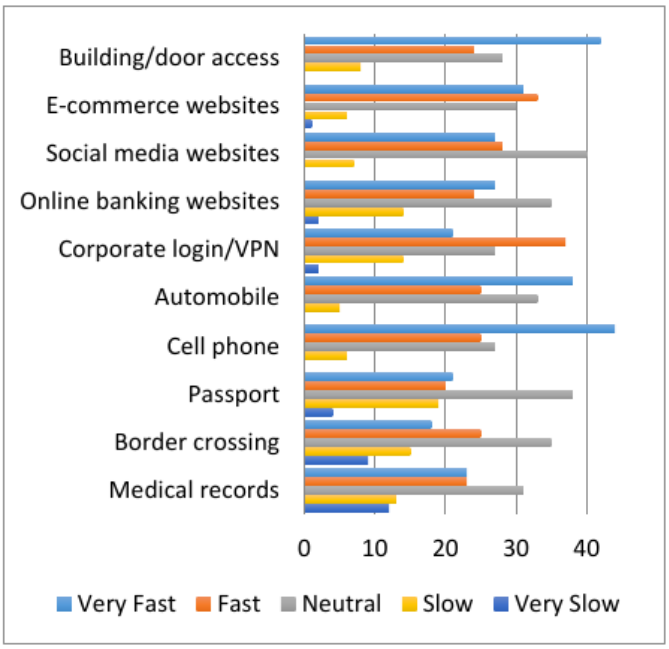

Fig. 7. Acceptable delay

The question was posed as to whether society was ready for the adoption of a biometric system. In the previous semester's survey, the respondents were split equally 50/50 on this matter but interestingly, this year, acceptance grew with 68% of the users willing to switch from a user-password combination to a biometric authentication system. (Fig. 8)

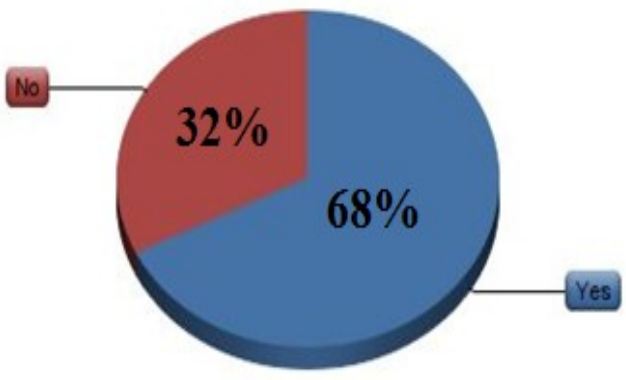

Fig. 8. Society acceptance

The respondents also agreed that a biometric authentication system with or without a pin code was more desirable then the use of a username/password or no security in place as all with regards to ease-of-use, convenience and security. (Fig. 9)

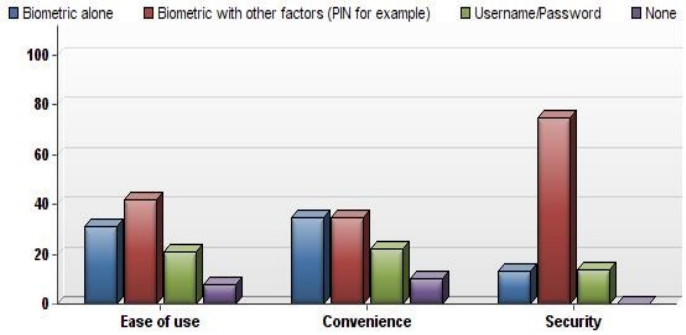

Fig. 9. Acceptability matrix

If a biometric system is to be adopted, it is important to know what types of biometrics would be acceptable to users. The following chart (Fig. 10) displays the multitude of different possible biometrics[2] and weather it would be acceptable for use. Fingerprint scan topped the list with 77% of respondents choosing that modality, most likely because it is well known and currently used in a number of biometric authentication systems. Facial, voice and speech recognition

Answer		Response	%
Fingerprint Scan		79	77%
Facial Recognition		74	73%
Voice Recognition		54	53%
Speech Recognition		50	49%
Palmprint Scan		41	40%
Retina Scan		41	40%
Keystroke Recognition		29	28%
Iris Scan		28	27%
Finger Geometry		27	26%
Hand Geometry		24	24%
Handwriting		12	12%
DNA		10	10%
Vein		7	7%
Ear		7	7%
Infrared Imaging/Thermographic Imaging		6	6%
Gait (Walk)		5	5%
None		2	2%

Fig. 10. Types of acceptable biometrics[2]

followed. These the modalities are the basis of the system designed by Recognition Technologies, Inc. More invasive techniques such as retina or iris scan, DNA and infrared imaging were less popular. Other methods such as finger, hand and ear geometry and gait which are less familiar to the public were chosen very little as well.

The client also desired to show the ease-of-use of the biometric authentication system by having a child use the device. The video included a scene with an 8 year old girl enrolling and utilizing the system. There were no issues and it worked as it was designed. The question was asked to the survey pool whether a biometric system was acceptable for use with children at home, school, home and school or not at all. The majority (56%) of respondents stated it was acceptable at home and school. 22% determined it was not an acceptable method for use with children.

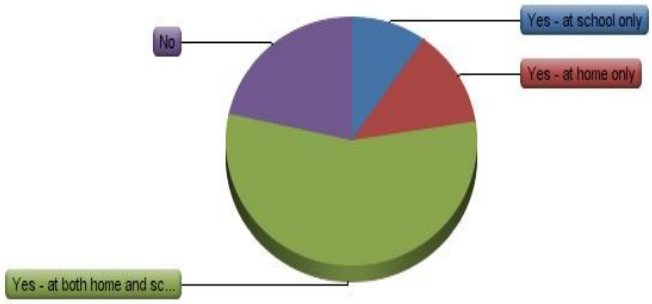

Fig. 11. Biometrics and Children

V. CONCLUSIONS

In the world of biometric security, the future "password" will be the user themselves. Virtually every market in the world has adopted the surge in use of biometric technology for individual identification. Biometrics is slowly replacing passwords, personal identification numbers (PINs), plastic ID cards, and other forms of what are considered antiquated and unsecure methods of authentication. Even though this all sounds exciting and cutting edge, we are still a few years away from this being an exact and precise solution. Team 2, when testing the technology ran into some issues of consistency and latency.

As the survey came to a closing after only being live for a short time, seven days to be exact. The limitation of the survey timeframe played a big role in the total number of responses collected. The core study team made of four members each targeted about 75 personal contacts, which included family, friends and co-workers as well as posting it on their social media sites if available. The survey also went to Pace University Capstone students and DPS candidates.

Regardless of the timeframe, the data collected doubled from the previous year, as 68% of the respondents indicating that society is ready for the standard user/password combination to be replaced with biometric systems. The top

four biometrics that the respondents are comfortable using are Fingerprint scan with 77%, Facial Recognition at 73%, Voice Recognition 54% and Speech Recognition at 49%. The study suggests that the top four biometrics preferences are due to the current technologies on cell phones, tablets and laptops which already integrates biometrics security technologies.

Next semester's study, the team should discuss with the client what a suitable percentage is needed as an acceptable/ease for the study. Also, a working model should be deployed so users could have hands on enrollment and testing capabilities. Having access to the system even on a limited basis could be of great help. While shooting the video, for the survey, the team should keep to a shorter timeline (5 mins). One of the observations from the surveyors was that the video was too long and kept going. While it isn't easy to fit all the necessary information into a five-minute video, the team should really decide on a storyline and timeline and decided what needs to make the video cut before the official shoot. Another issue the team would need to address with the client is the delay timing between the authentication and access being granted. It is also necessary to discuss thresholds of similarity in physical appearances and voice similarities. We were able to spoof the system up to a 40% threshold of similarity, which is concerning because, even though voice and facial patterns are unique there are still several similarities that can spoof a system similar to our experience.

Though not perfect and there are several concerns over security and transfer of sensitive information, biometric authentication is going to be a big part of our day-to-day lives in the very near future.

APPENDIX

Survey Questions:

1. *What is your gender?*
   - Male
   - Female

2. *How old are you? (You must be at least 18 years old to participate)*
   - 18-24
   - 25-32
   - 33-40
   - 41-55
   - 56+

3. *How many unique username and passwords do you think you use on a daily basis?*
   - 0-5
   - 6-10
   - 11-15
   - 16-20
   - 21+

4. *Please rate how convenient the audio and visual biometric verification appeared.*
   - Extremely convenient
   - Somewhat convenient
   - Neutral
   - Somewhat inconvenient
   - Extremely inconvenient

5. *Please rate how secure the audio and visual biometric verification appeared.*
   - Very secure
   - Secure
   - Neutral
   - Insecure
   - Very insecure

6. *Please rate how easy the audio and visual biometric verification appeared.*
   - Very easy
   - Easy
   - Neutral
   - Difficult
   - Very difficult

7. *Do you feel there was a delay in the verification system?*
   - Yes
   - No

8. *How much delay would be acceptable given the added security of the following applications? (This is a matrix of applications vs. delay)*

Application
   - Building/door access
   - E-commerce websites
   - Social media websites
   - Online banking websites
   - Corporate login/VPN
   - Automobile
   - Cell phone
   - Passport
   - Border crossing
   - Medical records

Responses
   - Very fast
   - Fast
   - Neutral
   - Slow
   - Very slow

9. Do you think society is ready for the standard user/password combination to be replaced with biometric systems?
   - Yes

- No

10. *Pick which verification system you would use if your goals were the Ease, Convenience and Security. (This is a matrix benefit vs. system)*

Benefit

- Ease of use
- Convenience
- Security

Verification System

- Biometric alone
- Biometric with other factors (PIN for example)
- Username/Password
- None

11. *Which of the following Biometrics would you be comfortable using. (Check all that apply)*

- Facial Recognition
- Hand Geometry
- Finger Geometry
- Fingerprint Scan
- Speech Recognition
- Retina Scan
- Keystroke Recognition
- Palm print Scan
- DNA
- Ear
- Handwriting
- Voice Recognition
- Vein
- Infrared Imaging/Thermographic Imaging
- Iris Scan
- Gait (Walk)
- None

12. Would you allow biometrics to be used with your children?

- Yes - at school only
- Yes - at home only
- Yes = at both home and school
- No

REFERENCES

[1] Homayoon Beigi, "Mobile Device Transaction Using Multi-Factor Authentication," USPTO publication No. **20120110341,** Filed November 2, 2011, Provisionally filed, November 2, 2010, Allowed March 23, 2015. URL:http://www.recognitiontechnologies.com/~beigi/homayoon/patents/20120110341/pat20120110341.pdf

[2] Homayoon Beigi, "Fundamentals of Speaker Recognition," Springer, New York, 2011, ISBN: 978-0-387-77591-3.

[3] Kresimir Delac and Mislav Grgic, "A Survey Of Biometric Recognition Methods", Elmar, June 2004: URL: http://researchweb.iiit.ac.in/~vandana/PAPERS/BASIC/survey.pdf

[4] Kai Li "Identity Authentication based on Audio Visual Biometrics: A Survey" URL:http://www.eecs.ucf.edu/~kaili/pdfs/survey_avbiometrics.pdf

[5] Synodinos, N. E., Papacostas, C. S., & Okimoto, G. M. (1994). Computer-administered vs. paperand-pencil surveys and the effect of sample selection. Behavior Research Methods, Instruments, and Computers, 26(4), 395-401.

[6] [4] Kiesler, S., & Sproull, L. S. (1986). Response effects in the electronic survey. Public Opinion Quarterly, 50, 402-413.

[7] Research Design and Data Collection, Chapter 8 "Survey Research URL: http://www.sagepub.com/upm-data/43589_8.pdf

[8] J. Justiniano, C. Javier, A. Blecher, and Homayoon Beigi ``Acceptability Research for Audio Visual Recognition Technology," Recognition Technologies Technical Report No. RTI-20150128-01, Jan. 2015, DOI: 10.13140/2.1.3521.0565.

[9] Charles Tappert, "IT691 Capstone Project – CS691 Computer Science Projects – CS389 Software Engineering" Spring 2015 URL: http://www.csis.pace.edu/~ctappert/it691-15spring