Acceptability Research for Audio Visual Recognition Technology

Recognition Technologies, Inc., U.S.A.

Technical Report: RTI-20150131-01

Jason Justiniano, Catherine Javier, and Alon Blecher
Seidenberg School of CSIS, Pace University, White Plains, New York

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

***Abstract* – Username/password is currently the standard for authentication. As the need for authentication increases, username/password authentication is becoming increasingly cumbersome. Additionally, it is becoming less secure. Biometrics could augment or supplant this standard. Existing research seeks to identify biometrics with the greatest opportunity and establish their security. However, there are few studies investigating preferences of biometrics compared to username/password. This study seeks to define an approach to assess preferences and collect qualitative results for biometrics as a replacement to username/password. Audio and visual recognition technology with a pin was compared to the standard of username/password. The online qualitative study had 52 respondents. Overall, biometrics scored highly for security, ease, and convenience in comparison to username/password. The results suggest there are places where biometrics would be a successful replacement to username/password, but would meet greater resistance in other aspects of users' lives.**

***Keywords* – Biometrics, Face Recognition, Visual Biometrics, Speaker Recognition, Multimodal Biometrics, Multifactor Authentication**

I. Introduction

"There is growing interest in biometric technology that leverages the sensors available on smart phones. These will be important in high volume verification applications like entitlements, banking, online purchasing, etc [1]." This quote, by Cambier, describes the increasing relevance of biometrics as a more convenient and secure method of accessing important information on devices, particularly smart phones. As the gateways to access information continue to proliferate, the use of username/password are becoming increasingly cumbersome and impede productivity in our mobile devices today.

Another dimension Cambier could have discussed is that biometrics recognition is becoming increasingly relevant to almost every aspect of society where verification and security are important, not just through smart phones. Our society has reached a point where the saturation of username/password for log in has caused us to be counterproductive. Moreover, this is not limited to access over the Internet. For example, we use security key cards to enter places, passwords to open doors, codes to open safes and pin numbers to purchase a wide variety of commerce. We even require verification for travel and at border crossings. This growing pressure results in a constant testing of the limits of the username and password paradigm. As such, it is important to explore the viability of newer, potentially more secure and more convenient access methods.

There are a number of Biometric methods in use today, the most popular being keystroke, ear, hand geometry, fingerprint, face, retina, and voice [2]. Each one of these contains a set of attributes that makes them unique. For example, fingerprints have minutiae points; voice has unique highs and lows, and faces have attributes of different shapes such as eyes, nose, lips, chin, eyebrows, and their spatial relationships [3].

Unimodal biometric systems installed in current applications have many limitations. These limitations can be overcome by combining two or more biometrics; which is called a multimodal biometric system. These systems are made more reliable by combining multiple independent pieces of evidence, running different types of recognition and verification systems [4].

A review of the literature revealed an abundance of study in the area of biometrics. A range of research strategies have been employed to investigate this area. Chetty conducted a quantitative study using trial and error to assess the security of various biometrics and biometric combinations [5]. Gorman conducted a qualitative study to explore different methods of identifying vulnerabilities in biometrics systems [6]. Bhattacharyya also conducted a quantitative study to explore the advantages and disadvantages of one biometric versus another. This study had a wealth of detail across the many forms of biometrics [7], and Jamieson assembled a review paper that took a longitudinal look at past research to determine insights for biometrics [8]. It is clear that the emphasis has been on establishing the security of biometrics. While, much of the research discussed that biometrics needed to functionally replace the current standard of username/password, there appears to be a significant gap in the analysis. Current research did not evaluate the

· *Published as a Recognition Technolgies Technical Report on Jan.31, 2015* acceptability and preference of biometrics as a replacement to username/password. Given the increased obstacles in replacing username/password this gap in the analysis is understandable. It is crucial to establish the viability of biometrics and its security.

As demonstrated in detail below, it is not immediately apparent which, if any, method will ultimately replace the current standards. Furthermore, in order for the new method to take hold and shape a new paradigm, the newer evolution must align to an evolution of the infrastructure in society. Given the entrenched nature of the current username and password standard, it is essential that significant and meaningful research be conducted to thoughtfully bring about change that is both relevant and welcomed. The research conducted below seeks to advance the knowledge in this area and considers preference from the user's point of view; thereby filling an important gap of knowledge.

II. Background

This study will be conducted in phases. The initial phase of this study (conducted in the fall semester of 2014) will consist of a qualitative survey to better understand current perception of audio and visual biometric technology. The goal of the study is to deliver valuable qualitative information, which will inform a phase 2 quantitative study (expected in the spring semester of 2015) to assess the acceptability of audio and visual biometric systems. An important goal is to assess what aspects of their daily lives users are willing to accept and possibly welcome biometric technology.

This study is being conducted in collaboration with Recognition Technologies, Inc., who has also contributed access to their proprietary audio and visual recognition system for use in this study. Recognition Technologies, Inc. is a biometric research company that is involved in the development of many different forms of biometric systems. These biometric systems include Speaker Recognition (Identification and Verification), Signature Verification, Speech Recognition and Handwriting Recognition (Identification and Verification) [2].

The software being used in this study is a multifactor authentication system. It uses cryptography and key factoring along with symmetric and asymmetric encryption. The software is based on the use of visual and audio biometrics. This software focuses on three main factors, as explained by Homayoon Beigi's, CEO of Recognition Technologies, Inc., patent [9]. These factors include "possession of an item, knowledge of a fact and the identity."[9] In our study the user will have "possession" of a mobile device, "knowledge" of a secret PIN and will provide their voice and visual appearance as "identity." The knowledge and identity information is provided when the user completes an enrollment process to use the audiovisual biometric system. Enrolling the users' biometrics in the system involves the creation of a pin number, and an audio/visual recording. For security purposes, the enrollment is verified by a third party using PKI (Possession, Knowledge, and Identity), and is certified by a SSL certificate authority. When using the software, the visual and voice biometrics have to be sent to the server. The server must recognize the person's biometrics and then will either provide access or send a declined notice back to the user. A score is assigned when trying to gain access [9].

Determining this course of study was a collaboration between the owner of Recognition Technologies, the Pace University DPS candidate, the professors of the capstone course and the core team registered for the capstone course. Originally, the experiment was supposed to be a quantitative study. However, due to time constraints, lack of budget, and the extended process of engaging with the software introduction the study was parsed into two phases. Additionally, it became apparent that the responsible course of research was to conduct an exploratory qualitative study, which will inform the more extensive quantitative study. This will assure that resource will be appropriately deployed in the spring of 2015. This will also provide phase two of the study with justification for resource allocation and study design. The goal for next semester's students is to turn the insights of this study into a quantitative experiment.

III. Methodology

A. Study Objective

Primary—Assess Audio Visual Biometric acceptability when applied to a hierarchy of real-world scenarios with different levels of sensitivities and importance.

Secondary—Gain anecdotal learnings into which facets of daily lives end-users are willing to accept and use biometric technology.

B. Target Population

- The current sample will be taken from a pool of Pace University students, faculty members, and possibly others outside of Pace University
- Next semester's study should aim to achieve a response rate high enough to allow for data analysis with significant result segments

C. Method for Data Collection

- Data collection will be achieved through a survey distributed via email
- There will be a brief video included as a part of the survey to provide foundational context which will help responses to be more comparable

Results will be received immediately upon completion of the survey, and stored in a dataset.

IV. Survey Design

To provide context and attempt to bring all potential respondents to a comparable level of understanding, we developed and included a four-minute video at the beginning of the survey. Homayoon Beigi begins the video with an introduction that describes the biometric software. Then the core research team demonstrates how to use the biometrics system to open a door. Several spoofing scenarios on the biometrics system were also demonstrated. It was also mentioned that if two people try spoofing the system and both were enabled, we both would have access to the system because the system is designed for groups of people to have access at one try. Throughout the video, viewers are able to see different screenshots of the application with visuals of the interface.

The video also establishes safety and security of the system. Whenever a person was enabled or disabled, the system operator had to go into the database itself to change the options as opposed to doing it with the application. This highlights security since not everyone has access to the database.

In order to create a well-designed survey we focused on: language, length, format, delivery method, and feedback. It was important that the survey questions were developed thoughtfully so as not to be biased. The structure of a survey is also important. The survey was designed in such a way that participants would hopefully be more willing to answer the questions. A review of the literature provided some best practice strategies, which were leveraged in the design of the survey.

Research showed that a well-written survey using simple and straightforward language helps the participants better understand the questions asked and therefore, they provide more accurate answers [10]. The length of the survey is also significant. Most participants would be less likely to complete a long survey. Our survey consists of 13 questions, which can be reviewed in the appendix of this study. The questions are presented in a single scrolling page. There is evidence that shows that participants are more likely to answer an online survey where they can scroll to answer the questions as opposed to paging through the questions [11]. Not only does presenting the survey in a single page give the participant an overview of the length of the survey, but also allows them to preview the format in which the questions are asked. Our survey questions are formatted as multiple-choice questions, which more people are willing to answer. Open-ended questions require more cognitive effort from participants [12]. Although, participants may still be willing to provide their feedback, open-ended questions can become lengthy resulting in loss of interest. This loss of interest affects the accuracy of the participant's answers. The delivery method of this survey is through e-mail. Having our participants' complete surveys through e-mail is a fast and efficient way to gather data. After creating questions and designing a user-friendly survey, we obtained feedback from Beigi to ensure the questions are unbiased and pertain to the targeted audience. Corrections were made to ensure that each question is clear, concise, and provides us with the trends and opinions we are looking for.

These questions focus on gathering data about how convenient and secure respondents feel the biometric system is after watching the video. It also asks respondents to compare the biometric system to the current standard, username/password. The questions asked leverage a number of traditional methods for ranking and scoring responses for later evaluation, an example of this is the Likert scale.

The study focuses on assessing the respondent's perception of the system's security, ease of use and convenience it may provide to common everyday activities where authentication is required or useful. The list included: E-commerce Website, Social Media Site, Banking Websites, Online Medical Records, Corporate login, Car, Home, Elevator Access, Building Access, Cell Phone, Passport, Border crossing, and Vending machines. This list was developed strategically to include a hierarchy of real-world scenarios with different levels of sensitivities and importance. This grouping was not apparent to the respondents; however, the study team will look for patterns in the responses to draw conclusions of the potential attitude of acceptability to biometric systems across the range of gateway studies. The cross section can then be used to make extrapolations to other gateways of access with similar security/convenience profiles as those in the study. Username and password was always provided and a control to use as a benchmark for comparison of the responses in the study.

The study concludes by seeking some anecdotal information about the respondents' attitudes around society's readiness for biometrics and their willingness to adopt biometrics for both themselves and their children.

V. Results and Findings

As the video and associated surveys were recently fielded and responses are still being collected, a full analysis of the results has yet to be completed. Below are some of the more intriguing early results. That will lead to more depth conclusion upon further analysis.

The survey was initially sent to the primary target at Pace University. Subsequently, the core study team sent the survey to colleagues and friends, and Beigi sent the survey to a combination of academic and professional colleagues at his same level. The responses were recorded in independent spreadsheets to allow for potential segmentation of the results. However, given the relatively small number of respondents, all the data was pooled together for a consolidated analysis. The results in this paper are from the 52-pooled respondents.

The first piece of data the study is gathered is age. When it comes to technology, different age groups can be either willing or less willing to adapt to a new technology such as audio and visual biometrics. Age provides an idea of how familiar the respondent may be with technology.

There were significantly more male respondents than female respondents, which can be seen in Fig. 1.

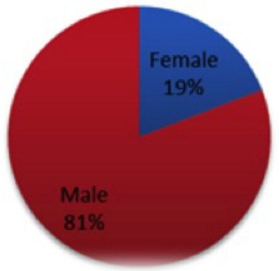

Fig. 1. Gender breakdown in the study.

There seemed to be an even distribution of age groups with a slight clustering in the 41-55 age group, as shown in Fig. 2.

The study gathered how frequently respondents used username and password on a daily basis, and how many unique username and passwords they used on a daily basis. The data seems to show that most users don't have more than 10 usernames/passwords, as shown in Fig. 3. There are some outliers that indicated greater than 21 usernames/ passwords. It is likely that due to the relatively small number of respondents that these patterns are not suggesting anything in the population. In future phases of the study, the patterns should be compared to see how an increase in the sample might change the interpretations.

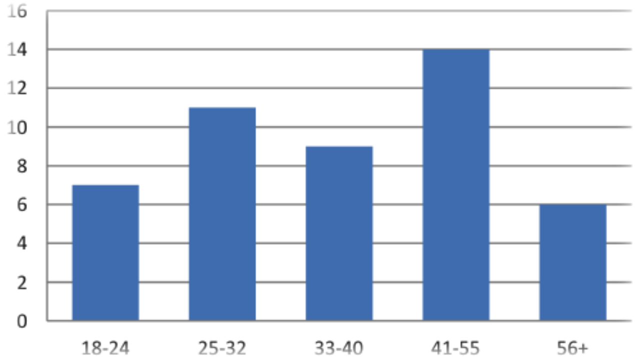

Fig. 2. The distribution of age grouping in the survey

The data also provides some baseline insight into what respondents' attitude is towards biometric after having watched the introductory video. 69% of people surveyed claimed that they would use biometrics for normal tasks, as shown if Fig 4. A segmentation of the data to look at the trends of older respondents (age 18-32 vs. ages 33- 56+) showed that the older segment was more likely to use biometrics in their daily lives than the younger segment, 72% vs 65% respectively.

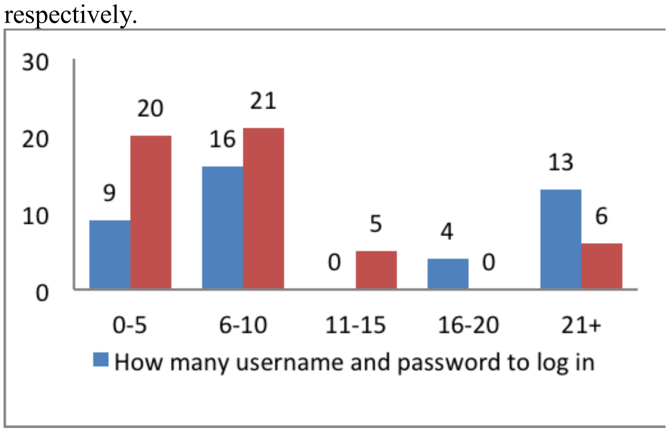

Fig. 3. Current frequency of username/password use

This is a counterintuitive finding when you consider the segmentation from the next two questions. The data shown in Fig. 5 and Fig. 6 below help provide an understanding of whether users would be willing to use biometrics.

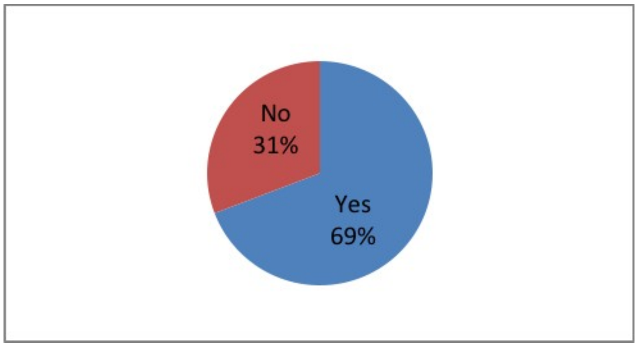

Fig 4. Would you use audio and visual biometrics for normal tasks?

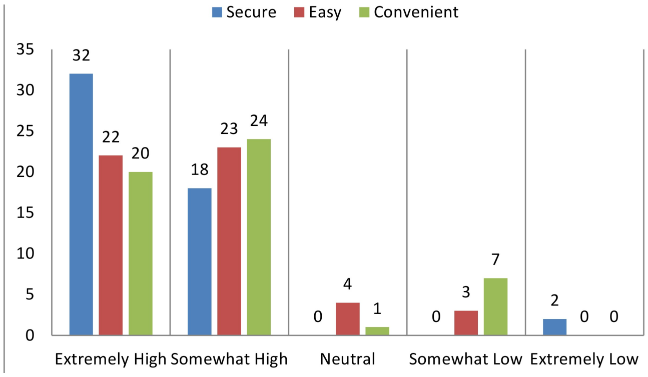

Fig. 5. Show how respondents ranked the biometric system as shown in the video in the following criteria; security, ease, and convenience

Data from Fig. 6 confirms some of the conclusions from Fig. 5, as we see clearly that biometrics scored highly for security, ease and convenience. This data does provide the insight that the addition of the PIN is reducing respondent's perception of the convenience and ease. We did a segmentation of the data to look at the trends of older respondents (age 18-32 vs. ages 33- 56+) and saw an interesting shift. For the younger segment (n=20) the majority of respondents felt the biometric system was "extremely" secure, easy, and convenient; 70%, 60%, and 50% respectively. For the older segment (n=32) the majority of respondents felt the biometric system was only "somewhat" secure, easy, and convenient; 56%, 50%, and 56% respectively. While these numbers come from a very small group of respondents, they confirm the natural inclination that the younger segment would be early adopters and suggests that further study is warranted to discern other differences in these segments. This data seems to contradict the data from question 10 in the survey. This is likely a result of the small sample size of the study. A study designed to generate greater respondents would be statistically powered to handle these population subsets.

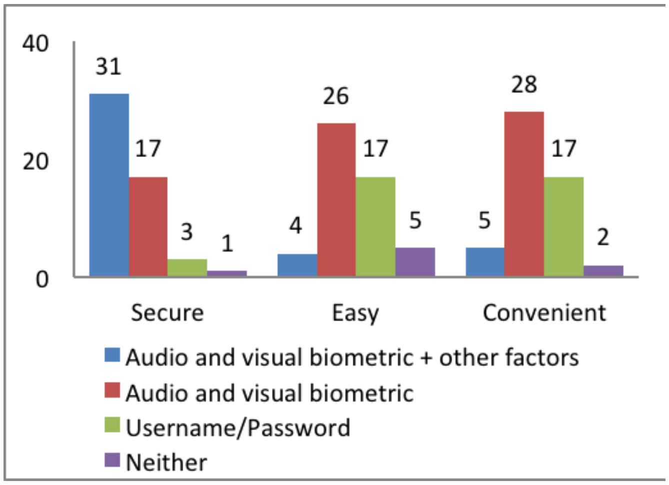

Fig. 6. Ranking of attitudes after watching the introduction video

The data in Fig 7. shows the overwhelming majority of respondents would prefer audio and visual biometrics over username and password for the traditional gateways online that require high security, such as banking websites or, online medical records. However username/password seems to still be a preferred method of access. In Fig. 8 it is shown that biometrics alone were selected and username/password does not seem to be represented for gateways which are not currently protected by username/passwords, but that could be fortified by biometrics. Examples from the study are building access and border crossing. This could suggest that because security is high and username/password is not currently used, no previous standard is impeding the adoption of biometrics. This could suggest that once users got over the initial experience of using biometrics the adoption could accelerate. This is an interesting topic for future study.

The responses for gateways that are more a matter of convenience than security, shown in Fig. 9, seemed to have a more distributed range of responses with no clear preference to biometrics or username/password. These are interesting findings and suggest that further research could be beneficial in this area to illuminate the barriers to biometrics.

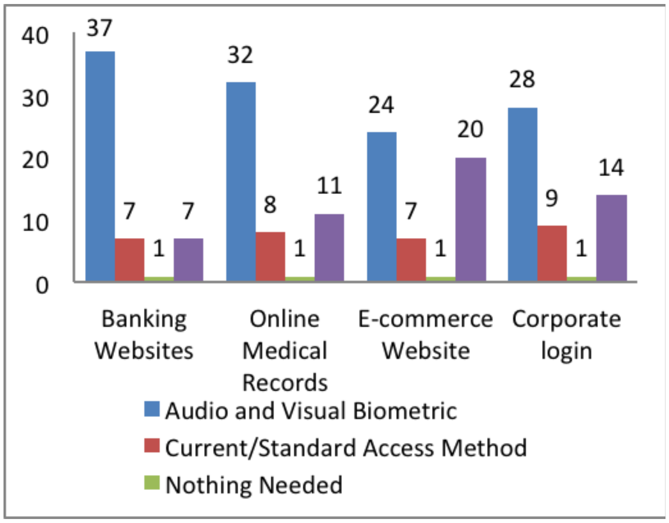

Fig. 7. Traditional gateways that currently use username/password for login that are considered to need the highest security

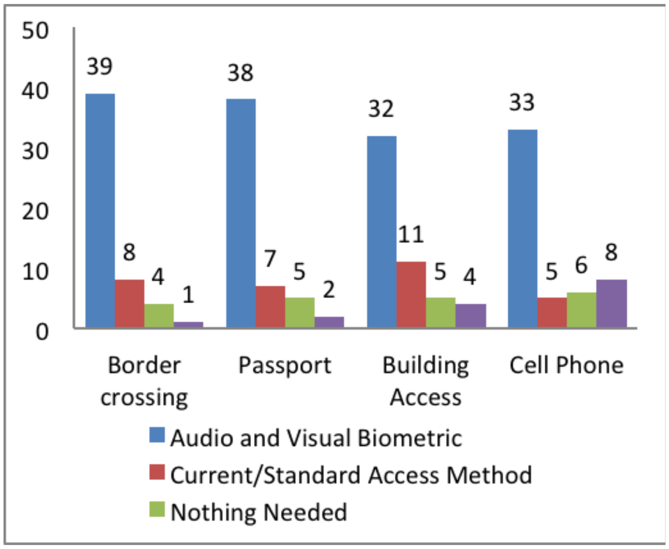

Fig. 8. Gateways that do not currently use username/password for login that are considered to need the highest security

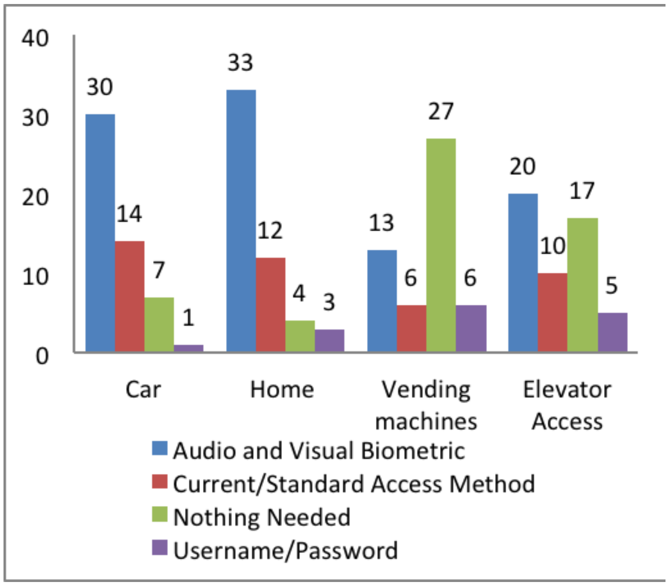

Fig. 9. Gateways that do not currently use username/password for login and where biometric could offer convenience

The results to question 9 in Fig. 10 clearly show a trend forming that face, speech and voice are the most accepted biometrics among the respondents, if one considers that speech and voice are really describing the same biometric. Fingerprint then becomes third. This is confirmation that the biometric systems use in the video are developed using the kinds of biometric that are most acceptable to users.

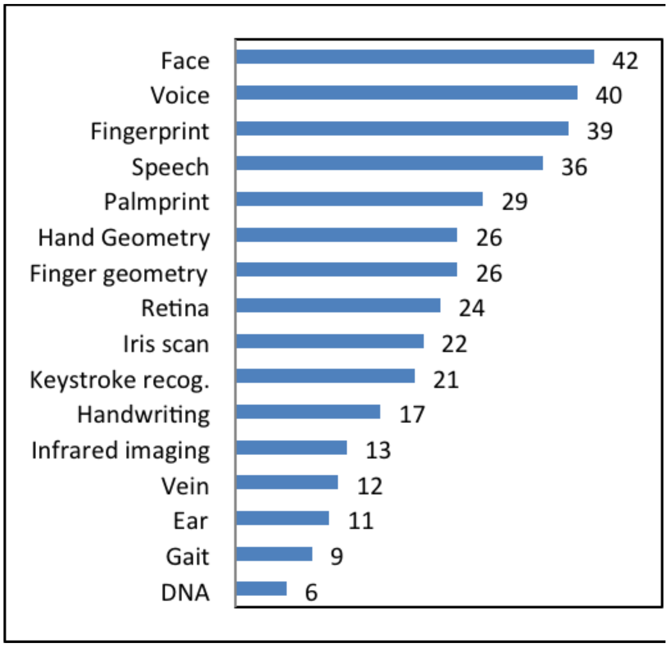

Fig. 10. Frequency of response to which biometrics the respondents would be willing to provide

There is nearly a perfect split about the respondent's attitudes about whether society was ready for biometrics to replace the current standard of username/password, as show in Fig. 11. As more data is fielded, it will be interesting to see how the segments answer the other questions in the survey to identify patterns. This also suggests a possible focus for future studies.

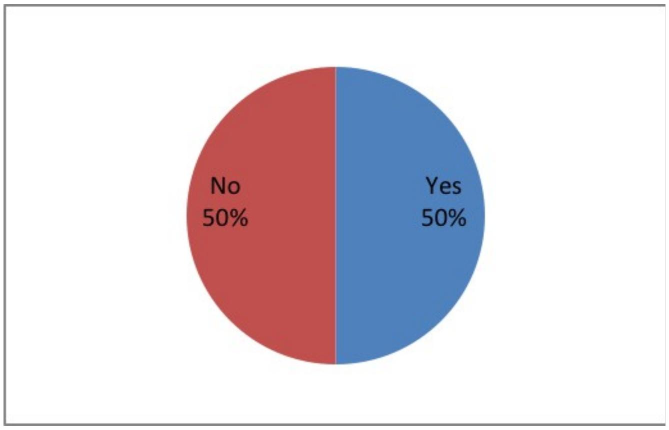

Fig. 11. Answer to question about society's willingness to accept biometrics today.

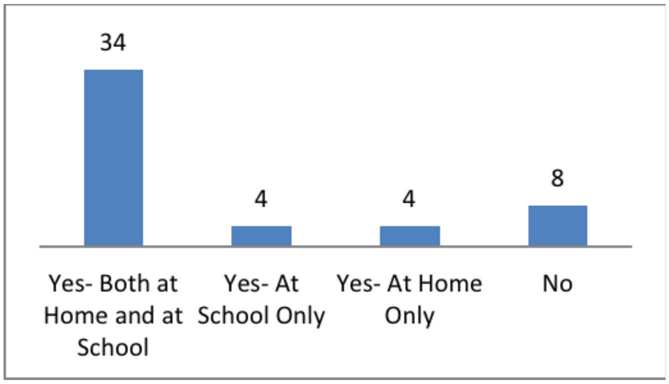

Fig. 12. Breakdown of answers to how the respondents felt about the use of biometrics with children

There seems to be a willingness to adopt biometrics for use with children both at home and at school as show in Fig. 12.

We did not ask how satisfying the wait times were because we ran the system on a three-year-old laptop through a wireless network. The wait time in the video was not representative of the real-case scenario. Under normal circumstances, the response would be almost immediate. That is the reason we did not ask whether the wait times were acceptable.

VI. Conclusions

The survey results have limitations as a result of the survey frame. First, the survey was sent to Pace university capstone student, clients and DPS candidates, which totaled only approximately 50 potential respondents. The value of segmenting the data with such a small sample size is limiting. Moreover, the results are skewed as the survey was only presented to an academic population. A more realistic sample would have consisted of a broader range of responders across many demographic categories. The team attempted to augment the results by also sending the survey to friends and family, Biegi also sent the survey to a number of his associates while maintaining their privacy. The study team generated unique survey links so that results could be assigned to the various groups for potential analysis in the future. The additional targets increased the responses by 150%. However the overall responses to the survey, which number at 52 individual responders and no more than 20 in any given population, are still well below level to achieve significance. The ability to make any definitive conclusion is also limited as the survey numbers are not significant in any segment or even when considering the entire results. The recommendation for the next phase of this study is to identify sample populations that will yield the appropriate demographic composition for the study and use incentives to achieve a higher response rate.

Despite the low responses, this study does suggest that there is strong user preference for the use of biometrics in many aspects of users' lives. Furthermore, the study suggests that the differences in the places where biometrics would be preferred, over username and password, could be categorized by security and convenience. This should help focus further biometric systems research and development. It also suggests that there are many places where users are more resistant to shifting away from username and passwords. Careful consideration should be given to the populations with preexisting tendencies to use username and password. This is probably the most interesting conclusion from the study, which provides new insight for future work. The context in which the biometric is used has a significant impact on how the user will respond. When designing future studies it will be imperative that careful consideration be given to where the biometric is implemented. The study shows that the kind of gateway can have significant impact on the results. Future studies should be cautious of pooling results when the biometric is implemented in dissimilar places. This study was not powered to discern why that is, but some possible hypotheses for this could be that there is not a clear understanding of the improvement biometrics would offer. Biometrics might be seen as an over engineered solution in some user cases, or some users are physiologically more resistant to change. It will be interesting to see how future research can explore this further. It would be prudent for the answers to these questions to be found so that the introduction of biometrics into the mainstream is as smooth and welcomed as possible. The potential benefits for biometrics as an improvement and replacement of username and password are significant. This can only be realized by a thoughtful and well-designed implementation of future biometric systems development and implementation.

Appendix

Survey questions:

1. Please select your gender.
   - Male
   - Female
2. Please select your age group.
   - 18-24
   - 25-32
   - 33-40
   - 41-55
   - 56+
3. How frequently do you use a username and password to log in on a daily basis?
   - 0-5
   - 6-10
   - 11-15
   - 16-20
   - 21+
4. How many unique username and password combinations do you use on a daily basis?
   - 0-5
   - 6-10
   - 11-15
   - 16-20
   - 21+
5. Please rate how convenient the audio and visual biometric verification appeared?
   - Extremely convenient
   - Somewhat convenient
   - Neutral
   - Somewhat inconvenient
   - Extremely inconvenient
6. Please rate how secure the audio and visual biometric verification appeared?
   - Extremely secure
   - Somewhat secure
   - Neutral
   - Somewhat secure
   - Extremely secure
7. Please rate how easy the audio and visual biometric verification appeared?
   - Extremely easy
   - Somewhat easy
   - Neutral
   - Somewhat easy
   - Extremely easy
8. Select which verification system you would use if your goals were the following: Security, Convenience, or Ease?
   - Audio and visual biometric
   - Username/Password
   - Audio and visual biometric + other factors
   - Neither
9. Select which verification system you would use if your goals were the following:
   - E-commerce Website
   - Social Media Site
   - Banking Websites
   - Online Medical Records
   - Corporate login
   - Car
   - Home
   - Elevator Access
   - Building Access
   - Cell Phone
   - Passport
   - Border crossing
   - Vending machines
10. Would you use audio and visual biometrics for your normal tasks?
    - Yes
    - No

11. Do you think society is ready for username/password to be replaced with biometric systems?
    - Yes
    - No
12. Which of the following Biometrics would you be comfortable using?
    - Face
    - Voice
    - Hand Geometry
    - Finger geometry
    - Fingerprint
    - Speech
    - Retina
    - Keystroke recognition
    - Palmprint
    - DNA
    - Ear
    - Handwriting
    - Vein
    - Infrared imaging/Thermographic Imaging
    - Iris scan
    - Gait
    - None
13. Would you allow biometrics to be used with your children
    - Yes- At School Only
    - Yes- At Home Only
    - Yes- Both at Home and at School
    - No
    - Other

References

[1] James L. Cambridge, VP and CTO, Iris Technology, Cross Match Technologies, USA, 2012; URL: http://www.planetbiometrics.com/article-details/i/1414/

[2] Homayoon Beigi, Fundamentals of Speaker Recognition, Springer, New York, 2011.

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

[4] L. I. Kuncheva, C.J. Whitaker, and C.A. Shipp, "Is Independence Good For Combining Classifiers" School of Informatics, University of Wales, Bangor Gwynedd LL57 1UT, UK, September, 2000;

[5] Girija Chetty and Michael Wagner, "Audio-Visual Multimodal Fusion for Biometric Person Authentication and Liveness Verification", *Human Computer Communication Laboratory School of Information Sciences and Engineering University of Canberra, Australia,* 2006.

[6] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", *Avaya Labs, Basking Ridge, NJ, USA,* 2003; URL: http://www.nikacp.com/images/10.1.1.200.3888.pdf

[7] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., and Minkyu Choi, "Biometric Authentication: A review", *Internation Journal of u- and e- Service, Science and Technology Vol.2, No.3, S*eptember, 2009;

[8] Roger Jamieson, Ph.D., Greg Stephens and Santhosh Kumar, "Fingerprint Identification: An Aid to the Authentication Process", *Information Systems Audit and Control Association,* 2005; URL: http://www.isaca.org/Journal/Past-Issues/2005/Volume-1/Documents/jopdf051-Fingerprint-Identification.pdf

[9] Homayoon Beigi, ``Mobile Device Transaction Using Multi-Factor Authentication,'' USPTO publication No. **20120110341,** Filed November 2, 2011, Provisionally filed, November 2, 2010. (http://www.recognitiontechnologies.com/~beigi/homayoon/patents/20120110341/pat20120110341.pdf)

[10] Martyn Shuttleworth, "Survey Research Design". *Explorable Psychology Experiments,* Jul 5, 2008.

[11] Aigul Mavletova, and Mick P Couper. "Mobile Web Survey Design: Scrolling Versus Paging, SMS Versus E-mail Invitations." *Journal of Survey Statistics and Methodology 2* 2012.

[12] "The Influence of Answer Box Format On Response Behavior On List-style Open-ended Questions." Journal of Survey Statistics and Methodology 2 (2014). Oxford Journals. Oxford University Press on Behalf of the American Association for Public Opinion Research. Web