My Finger, My Face, My Choice:

A Preliminary Study Exploring the use of Biometric Authentication on Mobile Devices and the Implications for Voter Verification

Imani N. Sherman, Brianna Posadas, Simone A. Smarr, Juan E.Gilbert
University of Florida
Human Experience Research Lab
Gainesville, FL
{shermani, bposadas, ssmarr, juan} @ufl.edu

ABSTRACT

Poll-workers in the United States of America play a critical role in the voting process. The decisions they make shape the experience voters have in the precinct, including the voter verification process. As politics waiver, the right to vote and the way in which poll-workers behave should not. However, changes in voter ID laws can affect how poll-workers carry out their duty, negatively affect voter turnout, increase the number of provisional ballots, and negatively affect minorities disproportionately. This research is the first step in a long term project to find usable solutions to the voter verification problem. We explore the authentication methods used on mobile devices and extract implications for voter verification. We conducted two separate studies: 1) to understand user authentication preferences for mobile devices and 2) to understand the usability of a new form of ID for voting. The mobile device study was completed via a survey while the voter ID study was a usability study conducted with participants and confederates. Our research shows that ease of use and speed are the deciding factors when mobile device users are choosing their authentication method, more so than security or privacy concerns. Also, voters were open to using a video as a form of ID at the polls. This leads us to believe that if a new form of voter ID, such as fingerprinting or facial recognition authentication or other processes available on smartphones today, were to be introduced, voters might accept it due to its ease of use and speed. This hypothesis will be tested in our next round of studies.

1. BACKGROUND

Authentication techniques, like passwords, smart cards, chips, PINs, and biometrics, are used to help ensure that only those who have been authorized can access an item. In voting, we use names, addresses, and drivers licenses to authenticate voter identity. Voter verification and related laws in the United States of America have changed over time. However, sometimes these changes lead to voter misunderstandings and increase the use of poll-worker discretion, thus affecting voting experiences [1].

1.1 Voting

Sometimes voters are turned away or delayed at the polls due to misinterpretation of the voter ID laws, forgetting the proper ID, and problems outside of the voters control. For example, in 2016, Syracuse, New York voters thought they registered at the Department of Motor Vehicles, but were somehow not registered, and were then turned away at the polls [8]. This resulted in voters appearing in Election Day Court to obtain court orders to vote. That same election proved problematic for Wisconsin when they introduced new voter ID laws in 2016 [2]. Older adults who had attempted to use other previously accepted forms of I.D., could not vote because they lost their license or tried to use an expired I.D. which was the case of one 85 year old woman. Research has shown that strict or complicated voter ID laws can impact voter turnout. In 2008, research done by Alvarez et al. showed that voter turn out was negatively impacted by stricter voter ID laws when compared to those with less strict laws in the 2000 and 2004 election and the 2000 and 2006 midterms [1]. Research done by Hanjal et al. showed that stricter voter ID laws negatively impacted nonwhites more so than whites [10]. In particular, Latinos were affected most negatively. There is a need for an authentication process at the precincts that is more accessible and usable for all voters.

1.2 Authentication on Mobile Devices

The use of authentication techniques have been reviewed, refined, and improved ever since humans needed a way to validate recipients of sensitive information. The use of systematic biometrics began in the 1800's with the use of fingerprints to identify criminals [4] and hand prints used to identify workers when they picked up their pay [15]. The introduction of biometrics for mobile devices has brought about a few interesting questions and scenarios. For example "If I use my face or finger to unlock my device, who else will have access to that information" or "If an officer of the law determines they need to unlock my device, can I be legally forced to use my finger or face to open it for them?".

However, just like changing voter ID laws, various technical authentication methods can lead to misunderstandings [12, 11]. These methods sometimes malfunction or lockout

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

a user with difficulty remembering their access code. Hang et al. found that most of their participants were locked out of an account due to difficulty remembering their password, while only a few attributed their previous lockouts to technical issues [11]. Kowtko found that the use of biometrics, CAPTCHA, and CAPTCHA alternatives may prove problematic for older adults as age and illness may affect accuracy [12].

When a user is selecting an authentication process, surprisingly security and privacy were not among the first features considered. De Luca et al. investigated the use of biometrics on Apple Touch ID and Android's Face Unlock [6]. Usability was the top reason users either activated, deactivated, or never used these methods. For users, trust and privacy were not among the decision making factors. Routi et al. conducted a usability study on authentication methods used online in 2015 [13]. Their results showed that users prefer single sign-on, transparency, and are intrigued by the use of biometrics. Although they prefer transparency in authentication, it also makes users trust the method less. The popularity of biometric authentication, despite its challenges, has led us to explore authentication preferences of mobile device users and determine the implications, and what we can apply, to voter verification.

To explore this, we conducted two separate studies. The first study, a mock election, compared the use of various forms of IDs and the implementation of vSquared, a video verification tool [7]. Participants found the use of a photo ID and video to be more useful when validating voters. The second study, a survey, gathered data on user's experience with mobile device authentication and the reasoning behind their current authentication method choice. Our results show that users prefer authentication methods that are easy to use and work quickly.This leads us to believe that the voter verification process, and the related laws, should be made simple and allow for other forms of ID to increase access to voting by being easy to understand and require less time. Our research suggests the use of video verification and fingerprint recognition to be methods worth investigating for further use. Although there are various reasons why a voter may be turned away from the polls, this paper will focus on voter verification issues.

This research is the first step in a long term project investigating ways to improve the voter verification process by looking at the success of authentication methods on mobile devices.

2. OBJECTIVES

The goal of this study is to explore the use of biometrics, specifically the fingerprint, as a method of authentication for mobile phone devices and determine the implications for voter verification. Our research questions are as follows:

1. How do we improve voter ID laws such that voter fraud is difficult but verification is easy?
2. Are there any similarities between difficulty found in mobile device authentication and voter verification?
3. How do we implement multimodal voter verification?
4. How do these usability preferences translate to voter verification?

We conducted two separate studies. The Mobile Device Authentication Study, discussed in Section 3, explored user authentication preferences for mobile devices. The vSquared Study, discussed in Section 4, investigated the usability of a new form of ID for voting.

3. MOBILE DEVICE AUTHENTICATION

This section will discuss the mobile authentication study.

3.1 Methodology

We created a Qualtrics survey of 83 questions, where the number of questions presented to a participant was dependent upon their answer to previous questions. The survey link was posted to the employee dashboard of a technology company and college students who wished to participate in the study signed up using a university research portal. Each student that expressed interest was emailed a personal survey link. Once they signed the consent form within the survey, they were then asked to complete the questionnaire. At the conclusion of their participation, each participant received extra credit from their teacher which was not to exceed 2% of their overall grade.

3.2 Participants

There were a total of 28 participants. 27 of those participants were college students, and 1 participant was not. Participants were between the ages 21 and 36 with 1 participant choosing not to provide their age. 46 % of participants were female and 54 % were males. Of the 28 participants, two participants do not currently use their fingerprint to log into their device. However, 6 % have used their fingerprint to log onto an iPad, 39 % on an iPhone, 48 % on an Android phone, and 6 % on a Windows Tablet .

3.3 Results

Authentication Method	% of Participants
PIN	96 %
Fingerprint	93 %
Password	86 %
Swipe-to-Unlock	79 %
Facial Recognition	39 %
Pattern	21 %
Voice Recognition	4 %
Iris Detection	4 %

Table 1: Percentage of participants that have experience using a particular authentication method to log-in to their mobile device

As shown in Table 3.3 most of the participants have experience using a Password,PIN and Fingerprint to authenticate themselves and unlock their device. It is possible that some participants misunderstood *password* as also being a *PIN* but we did not combine the two since it is possible for someone to use a *password* to unlock their mobile device. However, 68 % of participants currently use fingerprint or facial recognition, while 32 % of the participants currently use a non-biometric authentication method.

71 % either *Agree* or *Strongly Agree* that they would recommend their current method to a friend. When asked why they chose their method, convenience, speed, and safety were often referenced. For example, fingerprint users commented the following:

> It is quick, and fingerprints are unique to the user (even though recognition on some devices need to be updated)

> Because it is much faster than inputting my passcode. I am also able to unlock it while pulling my phone out of my pocket, which is impossible if you have to put in a passcode. By doing this the phone is already unlocked by the time I have it in position to actually use.

71 % of participants said it took them seconds or minutes to adapt to their current method.

For those who used fingerprint in the past, but currently use a different method, switched due to technical issues and changes in their mobile devices saying

> It detected everything as a fingerprint touch and locked me out.

> I changed phones and my new phone does not have this option.

. However, one participant found using the fingerprint to be cumbersome, saying

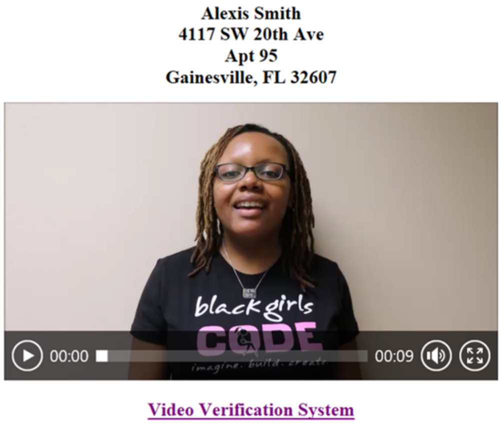
> I found the location of the sensor inconvenient especially if only one of your hands were free to hold the mobile. I just found it easier and faster swiping the lock screen with my thumb and then typing the pin.

4. VSQUARED

vSquared, a system designed by researchers in the Human Experience Research Lab at the University of Florida, allows poll-workers to verify voters using a video instead of a voter ID or license [7]. vSquared has not been implemented into the voting system. However, ideally a short video clip is recorded of the voter stating their name and address when they register to vote. This video clip will be used to verify the voter's identity on Election Day. It will also be updated at that time. The video itself contains a recording of the individual saying their name and address. A text display of the name and address of the voter is placed above the corresponding video frame. The video player has the following buttons: play, pause, volume control and expand video. An example of the vSquared concept can be seen in Figure 1.

4.1 Methodology

Participants were solicited from various classes at a university, and upon completion of the study would receive extra credit which was not to exceed 2 % of their overall grade. The participants were informed about the study and signed consent forms before starting the study. Each participant was told that they would be acting as a poll-worker during an election. Each poll-worker started by completing a demographic survey. Then they were introduced to a test voter, in order to acclimate them with their role and vSquared. Next, 12 voters (played by confederates) attempted to verify their identity and the poll-worker had to determine if they were allowed to vote. The voter would walk up to the poll-worker and hand over their form of identification (driver's license, voter identification card (without a photo), or vSquared). If using vSquared, the poll-worker would ask the voter to say their name and address. The poll-worker would then watch the video of the voter saying the same information and use that to verify identity. The poll-worker would then record if they would allow the voter to vote and why. Once all 12 voters attempted to vote, the poll-worker completed a survey about the use of identification. We did not use machine learning to conduct facial recognition in this study due to evidence that suggests humans are just as good, if not better, at facial and voice recognition when compared to machines [5, 14].



Alexis Smith
4117 SW 20th Ave
Apt 95
Gainesville, FL 32607

Video Verification System

Figure 1: Example of what would be seen when using the vSquared system for voter verification. The page includes a video of the voter saying their name and address and at the top of the page is the same name and address. Not shown, is the list of clickable voter's names that the poll-worker can search through.

4.2 Participants

19 college students participated in this study as poll-workers. 42.1 % of participants were female and 57.9 % were male. All participants were STEM majors between the ages 18 and 26.

4.3 Results

The 2015 vSquared study, conducted with 68 participants between the ages of 18 and 85, showed that poll-workers had a fraud detection rate of 78 % with vSquared, 8 % with a voter ID, and 7 % with a photo ID [7]. This result shows that it is easier for poll-workers to detect fraud when they have both audio and visual information to rely on and that users preferred vSquared for voter verification. Since voter fraud is seldom, the results here will focus on voter willingness to use a video instead of an identification card to vote and discover the successes and challenges of implementation.

When asked what type of identification is more accurate in verifying individuals for voting, 68 % of participants chose video verification, 32% chose photo ID card and no one thought using a voter ID card without a photo was accurate. When asked if they would participate in video verification, 74 % of participants were either *Willing* or *Very*

Willing to participate in video verification. However, only 42 % of participants said they would be *Willing* or Very Willing to use video verification for other applications (such as banking). There was no significant difference (p>.05) between the number of participants that were *Willing* or *Very Willing* to use video verification for voting when compared to those willing to use it for other applications.

4.4 Implementation

Before the start of the study, volunteer voters recorded videos for vSquared in a quiet room with neutral colored walls to use for the background of the video. We used a Canon EOS Rebel T5 camera to record the videos which took at most 5 minutes per voter. Before each “shift,” poll-workers were taught how to use vSquared and how to verify the identity of voters. Poll workers were told to first make sure the voters name appeared on the voter roll, listen to the voter say their name and address , then listen to the their video and determine validity. However, even after successfully completing a test run, poll-workers had issues using the equipment and 26 % of the poll-workers began using their own verification rules. For example, a few poll-workers also asked for a second form of identification. Reasons for false negatives included changes in hair style and misstating an address.

5. DISCUSSION

What did we learn from the mobile device authentication that can be used for voter verification? The results of the mobile device authentication study suggests that users prefer authentication methods that are easy to use and take a short amount of time. These preliminary results lead us to believe that younger voters may be open to utilizing new forms of authentication for voting as long as they improve the time it takes to check-in to vote and it doesn’t require as much effort. Although research shows that voter verification is one of the factors that cause a long line at the polls [9], no work has been done to determine if video verification or fingerprint recognition is quicker than using a typical form of ID. The Associated Press’s article discusses multiple accounts of voters losing and misplacing IDs, using the wrong ID, or an expired ID [2]. However, vSquared would require the voter to make a new video every so often, just like with their license, but they would not be required to carry anything to the polls. If a fingerprint was used, it would only need to be recorded once. But as mentioned by a few participants in the study, fingerprint authentication becomes difficult when the finger is wet or cold, not to mention when it is injured or missing. Therefore, we suggest allowing additional forms of ID for voter verification that do not require bringing a card or additional paperwork to the precinct.

5.1 Implementation

The vSquared study showed that majority of our poll workers would be willing to use a video for voting. However, just like other authentication methods, there are challenges with using vSquared. Implementing vSquared would add a video taking process to voters to-do list, which as previously mentioned, should not take much time. However, creating the videos themselves can be a serious undertaking for an election commission. It requires quality video and sound equipment along with a safe and secure storage location for the videos created. In our study, all poll-workers had access to the same database. For cities with limited budgets, this may be difficult to implement. Also, just like with a photo ID, the change of a hairstyle, weight, or skin color could potentially affect the poll-workers ability to correctly validate a voter based on the video. The use of a video would also require that poll-workers that check voters in to have the ability to hear, see and basic technical skills. This would require precincts to have quality headphones, laptops to watch the videos, and poll-workers that know how to use these tools. With majority of poll-workers being over the age of 60, the design of vSquared may need to change.

5.2 The Role of Voter ID Laws

Atkenson et al. point out that poll-workers are street-level bureaucrats who can use their discretion to verify voters [3]. In their study, poll-workers who believed a photo ID should be given for voter verification were more likely to ask for it even though it wasn’t necessary, per the laws of New Mexico. They found that poll-workers will be likely to use their discretion when checking voters identity when the voter ID law is complicated. And unfortunately this discretion negatively affects minority groups disproportionately. This research shows the importance of simple voter ID laws in order to keep voter fraud low but make the verification process easier for voters and poll workers. In vSquared, the poll-workers were told to ask voters to state their name and address when they used vSquared. However, this did not stop some poll-workers from asking for more information or another form of identification. For our study, the change in the voter ID law from they were used to, is likely to have caused this confusion. This leads us to believe that simple laws work as long as poll-workers completely understand how to use them.

6. CONCLUSION

Strict voter identification laws need to include forms of identification that allow registered voters without the typical voter identification card to vote. The results of the vSquared study show that young voters (16-26) may be open to a new method of verification via video. The Mobile Device Authentication study shows that the use of biometrics is becoming popular due to its ease of use and ability to save time. From this we learned that the ease of use and speed are important to authentication and should be taken into consideration for voting verification.No authentication method is perfect.There are implementation challenges and privacy issues with any form of identification. However, more authentication choices could improve voter experience and turn out.

6.1 Limitations

- These studies are limited by the small number of participants and the high percentage of college student participants.
- The study did not investigate the fact that utilizing a new form identification like a fingerprint or video bring about other security and privacy problems that would need to be addressed. For example, each precinct would need to keep all of the data private and ensure that it is not used by unauthorized parties.
- In the vSquared study, the poll workers gave their opinion of vSquared, but the voice of the confederates was missing.We did not showcase their view on creating and then using vSquared.

6.2 Future Work

As previously stated, this is the first study in an ongoing project to determine the preferred methods of authentication for mobile devices and use it to determine the implications for voter verification. The results of this study are limited by the small number of participants and the high percentage of college student participants in both studies. The next step in the study is to conduct a large scale survey, with a mixed population, that inquires about voting experiences and the participants willingness to use other forms of authentication at the polls and other locations. Our next study will evaluate user preference, willingness to use biometrics to vote, and the role security plays in participant choices. In addition, more work will be done to compare vSquared to traditional voter verification methods on time required, accuracy, and usability from voters to poll-workers.

7. REFERENCES

[1] R. M. Alvarez, D. Bailey, and J. Katz. The effect of voter identification laws on turnout. 2008.

[2] Associated Press. Wisconsin voter id law proved insurmountable for many voters.

[3] L. R. Atkeson, Y. P. Kerevel, R. M. Alvarez, and T. E. Hall. Who asks for voter identification? explaining poll-worker discretion. *The Journal of Politics*, 76(4):944–957, 2014.

[4] A. Bertillon. *Identification Anthropométrique: Instructions Signalétiques*, volume 1. Impr. administrative, 1893.

[5] V. Bruce, Z. Henderson, K. Greenwood, P. J. Hancock, A. M. Burton, and P. Miller. Verification of face identities from images captured on video. *Journal of Experimental Psychology: Applied*, 5(4):339, 1999.

[6] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann. I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1411–1414. ACM, 2015.

[7] J. Dunbar, P. Hall Jr, D. Moon, and J. E. Gilbert. Video verification: An alternative form of identify verification. *Procedia Manufacturing*, 3:4914–4920, 2015.

[8] M. Eisenstadt. Many people turned away from the polls thought they registered through the dmv.

[9] C. Famighetti. Long voting lines: Explained. *Brennan Center for Justice*, 2016.

[10] Z. Hajnal, N. Lajevardi, and L. Nielson. Voter identification laws and the suppression of minority votes. *The Journal of Politics*, 79(2):363–379, 2017.

[11] A. Hang, A. De Luca, E. Von Zezschwitz, M. Demmler, and H. Hussmann. Locked your phone? buy a new one? from tales of fallback authentication on smartphones to actual concepts. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 295–305. ACM, 2015.

[12] M. A. Kowtko. Biometric authentication for older adults. In *Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island*, pages 1–6. IEEE, 2014.

[13] S. Ruoti, B. Roberts, and K. Seamons. Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th International Conference on World Wide Web*, pages 916–926. International World Wide Web Conferences Steering Committee, 2015.

[14] O. Scharenborg and M. Cooke. Comparing human and machine recognition performance on a vcv corpus. 2008.

[15] G. Sodhi and J. Kaur. Indian civilization and the science of fingerprinting. 2003.