Critical Challenge Project: Final Report

"Use of a mobile device app for voting and its challenges"

SHUBHA DAHAL

Executive Master in Cybersecurity, Brown University

Advisor: Professor Roberto Tamassia

April 2020

ACKNOWLEDGEMENTS

I humbly thank my thesis advisor, Dr. Roberto Tamassia, Plastech Professor of Computer Science and Executive Director, Executive Master in Cybersecurity at Brown University, for providing me the opportunity to pursue this topic and for his continued mentorship, guidance, and support to me throughout the program at Brown. I thank my parents, my father, Mr. Tara Nath Dahal, and my mother, Mrs. Laxmi Dahal, for always believing in me and encouraging me to explore new opportunities and progressions in my life. I emphasize my profound gratitude and love to my spouse, Ms. Akshaya Bhattarai, for her unconditional love and support, and her constant words of encouragement, without which I would not have been able to complete my thesis. I express my gratitude to Ms. Dawn Reed, Administrative Assistant, Computer Science Department, Brown University, for ensuring that my thesis update meetings were timely and on schedule. Finally, I thank Brown University's Executive of Master in Cybersecurity (EMCS) faculty, staff, and my fellow amazing classmates (Fancybears) at EMCS Class of 2020.

Contents

Executive Summary

Voting is one of the most important rights of American citizens. Traditional voting methods used in the past elections lacked integrity, vulnerability to hacks, and manipulation. Despite its ease of using paper ballots for regular and absentee voting, studies have shown paper ballots are highly prone to fraud. Since the early nineteenth century, election fraud in the U.S. has been prevalent and still exists today.

In recent years, paper ballots have been complemented with mobile app-based ballots in some exceptional cases. States such as West Virginia, Colorado, and Utah have piloted a blockchain-based app for global ballot access to its military members overseas. Moreover, some states have introduced online or app-based voting as a testbed.

A study on the use of a mobile app in the 2018 West Virginia primaries found that when given an online voting option, voters abroad were 6% to 9% more likely to request a ballot and 3% to 5% more likely to cast it. Thus, mobile voting could have a powerful effect on voter turnout while drastically lowering the cost of voting. However, a study in 2020 found that the Voatz app was prone to cyber-attacks, and adversaries could discover a user's vote and disrupt transmissions. Furthermore, adversaries could potentially observe, alter, and add votes as they pleased.

Today, over 81% of Americans own a smartphone, and their reliance on smartphones is increasing, and so is the need for app-based mobile voting to supplement existing voting methods and to provide a more accessible solution to Americans living overseas. Current banking app's technologies, which maintain strict regulatory and banking industry-specific security standards to protect customer's personal and financial data, could be leveraged to authenticate and confirm the identity of a user, then vector access to mobile voting app. Banks have to comply with the REAL ID Act, which requires customers to produce proofs of identification and legal residency status in the U.S. We found 71% of Americans who used mobile banking applications found their personal information to be safe or somewhat safe using mobile banking. Opposingly though, we also found that most Americans still expressed the lowest confidence in online voting. But there seems to be a slow but a steady increase of users who find their personal information to be safe while using mobile banking

A voting app has severe critical cybersecurity challenges and limitations surrounding the app's security and transparency, voter privacy, and vote integrity. We realized that as a nation, we are not yet ready to fully utilize the mobile voting app in place of traditional voting methods.

We recommend the use of banking apps for identity verification of voters before they access the voting app, which should go through rigorous stress testing, development, and mock trials before its release. In order to amass public support and confidence, we propose the creation of a public-private partnership tasked to develop and support a cradle-to-grave system for the voting app while safeguarding voter privacy and vote integrity and providing education and training to the public. Finally, we recommend the introduction of the app gradually in small pilot programs throughout the U.S, which could inevitably become an effective alternative to traditional voting methods.

Background

This project was inspired and motivated by reading about West Virginia state using an app-based platform as a pilot program for its 2018 primary elections. West Virginia used a platform by Voatz, a Massachusetts company, and offered the app only to the West Virginians living overseas, primarily military members. Prior to that, it had never crossed our mind that this could be a possibility. After reading more, we started to wonder whether this could be the future of elections, not just in the United States, but all around the world. With almost everyone owning a smartphone or some smart device within reach of their fingertips, and the seamless internet connectivity enjoyed by all, we felt that it was just a matter of time until nations, including the U.S., enabled and incorporated the usage of mobile app-based voting.

We assumed that we knew that as a nation, we were not ready just yet to accept voting via the use of an app. Furthermore, the timing could not have been worse as we were learning about Russia's activities to jeopardize our presidential elections. We also wanted to learn more about the cybersecurity risks surrounding the use of such mobile-based apps and of previous research conducted to show the feasibility and usage.

Goal

The goal of this project is to research facts and explore the feasibility of the usage of an app on a mobile device for all elections, federal, state, and local. Specific objectives are as follows: overview lessons learned from the use of the Voatz app during the 2018 primary elections in West Virginia; analyze historical voter fraud trends, convictions, and how voter fraud has impacted the overall outcome of elections; identify cybersecurity risks associated with the use of a mobile-based app; and determine whether a mobile device voting app is suitable for elections today.

Approach

We focused our project just on the U.S. elections. More states these days are open to the idea of using an app for voting. Our activities primarily consisted of reviewing articles in journals and other scholarly venues, professional publications, government reports, and laws and judicial opinions.

Our work started with a detailed study of West Virginia's pilot program. In particular, we researched technical information on the app by Voatz used during the pilot program and how the app was introduced and distributed to the West Virginians living overseas.

Our focus then turned into finding historical data on voter fraud within the United States. The search led to finding a sampling of past election fraud data, including criminal convictions. Furthermore, we looked into possible the results of the election fraud and how the fraud had impacted the overall election. The court cases showed evidence of past voter fraud and

convictions. Further, the readings identified the vulnerabilities within the voting processes, including but not limited to voting registration, ballot casting, and ballot counting.

Research by University of Chicago Associate Professor Anthony Fowler on the use of the Voatz app and its outcome helped us understand how the app directly impacted the overall voter turnout, and how it aided in voting for military members stationed overseas. It also helped us understand the accessibility of votes because of the Voatz app.

Furthermore, we reviewed factors such as how the opportunity to use the app was distributed to the West Virginian voters, how their identities were authenticated, what were some risks and mitigation strategies, and what were some of the human factors which affected the pilot program.

We did not conduct interviews, surveys, or polls to gather data sets for this thesis. We reviewed online journals and past research on the use of similar technologies in sectors such as banking, the public's perception and confidence in using apps for banking, and the future feasibility of the use of an app for elections. The project was solely based on readings and reviews of past research, studies, and analysis. We noticed several security risks, identified limitations, and recommended possible mitigation strategies.

The approach was open to yielding either a favorable or unfavorable recommendation towards the use of an app-based voting platform for elections.

Research Findings

Election and Voter Fraud in the United States

Election fraud in the United States has been prevalent since the early nineteenth century. "Big-city" bosses in cities such as New York and Philadelphia did not shy about consolidating their powers by loading up their supporters with beer, arranging for them to vote under several aliases at different polling locations, kidnapping key officials working for the opposition, and scaring away their supporters with bare-knuckled street brawls [1].

The United States has seen its fair share of proven instances of voter fraud. In a sampling of election fraud cases within the United States, there were 1,088 proven instances of voter fraud. Out of which, in 949 cases, criminal convictions were secured where in which defendants either entered a plea of guilty or no contest or were found guilty in court or election-related offenses. Furthermore, 48 were civil penalties where defendants had to either pay fines or other penalties for violation of election laws [2]. Voter fraud mostly included:

i. Impersonation fraud at the polls: This happens when voting is conducted in the name of other legitimate voters, voters who have deceased, moved away or lost their right to vote because they are felons, but remain registered.

ii. False Registrations: Voting occurs under fraudulent voter registrations that either use a fake name and a real or a fake address or claim residence in a particular jurisdiction where the registered voter does not live and is not entitled to vote.

iii. Duplicate Voting: This occurs when an individual registers to vote in multiple locations and votes in the same election in multiple jurisdictions or states.

iv. Fraudulent use of absentee ballots: This occurs when individuals request absentee ballots and vote without the knowledge of the actual, registered voters; or obtains the absentee ballot from a voter or either by filing it directly in and forging the voter's signature or illegally telling the voter whom to vote.

v. Buying Votes: This transpires when voters are paid to cast a vote either in an absentee ballot or in-person for a specific candidate

vi. Illegal "Assistance" at the polls: This occurs when voters are forced, intimidated, or coaxed into voting for a specific candidate while supposedly providing them "assistance" with voting. The elderly, disabled, illiterate, and groups for whom English is a second language, are victim to this effort.

vii. Ineligible voting: This occurs when ineligible individuals such as non-U.S. citizens or convicted felons illegally register as eligible voters and cast their vote.

viii. Altering the vote count: This is when the actual vote count is changed either in a precinct or at the central location where votes are counted.

ix. Ballot petition fraud: This occurs when signatures are forged of registered voters on the ballot petitions, which must be filed with election officials in some states or issues to be listed on the official ballot.

Between 1976 and 1982, a grand jury uncovered a 14-year long systematic and widespread fraud in the primaries in two of New York's borough's Congressional districts. In one state legislative race, approximately 2,000 fake registrants were discovered, and in another about 1,000. Also, they found that one person had voted at least ten times in the year 1970, and in another, a team of six to eight fake voters cast up to a total of 100 fraudulent ballots in a primary election. Of the schemes, one was the registration of dead people or those who recently moved and registering in their names and casting an absentee ballot confidently knowing that these people would not come to the polls at all. The outcome resulted in affecting at least one election race [3].

In 1998, in Alabama, a police officer was convicted on seven counts of illegal absentee voting, wherein which the police officer and his accomplice forged absentee ballot request forms in the name of other voters, took them to the voters and obtained the signatures of the voters, unbeknownst to them that they were signing on their absentee ballots [2]. They then cast the ballot themselves. Later testimonies of multiple witnesses showed that the police officer went to their homes, told them to sign the absentee ballot for themselves and their children. At times the witnesses did not give permission or authorize Evans to complete, or to sign the application or affidavit, or to check a box on the application indicating they would be out of town on election day [4].

Also, in 1998, citing "a pattern of fraudulent, intentional and criminal conduct" in the casting of absentee ballots, a Florida Circuit Court Judge voided Miami's mayoral election affecting 360,000 Miami residents. A two-week grand jury trial which heard from over 60 witnesses' testimonies that the absentee ballots cast in the election included from people who did not vote,

who did not live in Miami or the district in which their ballot was cast, and did not qualify as unable to vote at the polls. Several ballots were doctored to alter a vote favoring one candidate, Mr. Suarez, who had long served as a Mayor of Miami from 1985 to 1993. The judge's ruling overturned his win, which was by over 2,800 votes [5].

Between 2001 and 2015, several states from Connecticut to Georgia, and Arizona to Illinois, individuals participated in absentee ballot fraud, tampered with the integrity of the absentee ballot, illegally signed and submitted ballot request forms for someone else, illegally "assisted" voters to fill out their absentee ballots, attempted illegal voting by casting ballots in multiple states for the same election, and registered to vote despite being ineligible to vote [2]. In some cases, even officials in the small town of Cudahy took part in a widespread corruption scheme that included accepting cash bribes and threw out absentee ballots that favored election challengers. After an investigation by the Federal Bureau of Investigation into the 2007 and 2009 elections, Angel Perales, the former head of code enforcement, admitted to tampering with mail-in ballots in city elections by opening them and then resealing and submitting votes for incumbent candidates while discarding for challengers [2]. Whereas, in 2013, Kimberly Readus, an Executive Committee member of the Canton City Elections, was convicted of stealing a ballot box [2]. Other ways of voter and voting fraud included of an individual who filled out voters' ballots for voters and told them for whom to vote resulting in the commissioner of Dothan City's election win, despite losing the in-person vote by a wide margin, won the election by an incredible 96 percent of the vote [2].

As observed above, the United States traditionally has had numerous voting and voter fraud incidents, which have led to severe fines and jail time.

Previous Use of App-Based Mobile Voting

In an unprecedented step in the United States history, for the first time in November 2018 general elections, the state of West Virginia implemented the option of using app-based voting which allowed West Virginia voters, specifically eligible West Virginians living overseas and uniformed services members, to cast their vote using an app. West Virginia introduced this pilot project to enhance ballot accessibility. It was the first-time mobile voting application, and blockchain technology was used in a federal election. Substantial security requirements, including utilization of federal standards for software development, regular maintenance and security upgrades, in-depth penetration testing, source code auditing, and audits of system's cloud infrastructures, were conducted and surpassed before moving the pilot program forward [6].

The option to use the app-based voting was extended to eligible uniformed services members and eligible voters in overseas countries for 24 counties, who had the option to vote either on their cell phone or their mobile tablet. Eligible voters were made aware of the app's availability when they received their mailings from the Federal Voting Assistance Program, which facilitated ballot access for registered U.S. voters residing abroad. West Virginia required eligible individuals first to sign a paper form, submit it via mail fax, or by scanning and emailing in order to submit a Federal Post Card Application (FPCA), according to the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) before utilizing mobile voting [7]. The app, which

utilized biometric facial recognition software and thumbprint safeguards to ensure the identity of the voter, increased the confidence of the auditors. Eligible voters used the app-based out of six different counties. Several reputable technology audit companies independently conducted Post-election security audits, and it proved that the technology provided a secure platform for voting and an alternative to the traditional absentee paper ballot [6].

One hundred forty-four voters, many of whom were active-duty members deployed overseas, used an app created by the Boston-based company Voatz, to make their choices in races for the U.S. Senate, the House of Representatives, states, and local offices [7]. The app used multifactor authentication and facial recognition to allow eligible users to access and then submit the ballots. Once a ballot was filled out, the app generated a PDF copy for the users, with duplicate copies sent back to the Voatz team and the relevant county election board. All ballots cast in West Virginia were backed up with paper records [7]. West Virginia also got a relative surge of interest when the Air Force sent an email to its active-duty members from West Virginia [7].

Since its first use, the Votaz app has been used during the 2019 City/County of Denver Municipal General Elections and the 2019 City/County of Denver Municipal Runoff Elections [8]. More recently, Utah County piloted the Voatz app to allow military absentee voters and their families living overseas to vote in a municipal primary election. The pilot was a collaboration between the Utah County Elections Division, Tusk Philanthropies, the National Cybersecurity Center, and Voatz [8]. However, this was a pilot program that was limited primarily to military members stationed overseas, who had access to secure internet connections and had adequate training to use the app and information security training.

While Voatz's app was introduced to replicate or replace existing voting machines, the Democratic Caucus in February 2020, in Iowa, introduced a new smartphone app to collect the result of its caucuses in order to let the party get the voting count to the public in an expedient manner. The app, developed by Shadow Inc., was to be used by party officials after tallying the votes and uploading them directly into the app to report it back. However, the app failed to do because several officials were unable to log into the app, and others cited that the app only reported partial data, which made the public cast doubt on the app's accuracy and integrity [9]. While the Department of Homeland Security did not have any reporting of malicious cyber activity against the app, it appeared that the app was not stress-tested to sustain the same volume of data as the election day. Several democratic party officials who were authorized to login and upload data into the app were not provided adequate training or did not know how to access the app.

Furthermore, some officials had not downloaded the app and practiced before, and some only downloaded it on the day of the election. Additionally, it appeared that the app was acquired only a few months before the use date [9], and it could be assumed that there was not enough time allocated for the development of the app's software and testing of the app to weed out any technical flaws before the election day. As a result, panic ensued on election day, and counties had to resort to traditional communication methods, such as telephone and paper, to report on their data.

Review of Voatz app use in 2018 West Virginia Primary Elections

Voter turnout is often low and unequal, but the opportunity to cast votes on a mobile device could drastically lower the cost of a democratic population. Implementing a differences-in-differences design with individual-level administrative data, Associate Professor Anthony Fowler at the University of Chicago's Harris School of Public Policy studied West Virginia's trial with mobile voting in 2018 to see what happens when Americans have the opportunity to vote online. He utilized administrative data and the fact that mobile voting was only available for overseas residents for the residents of some West Virginia counties. He found that when West Virginia's registered voters living abroad had the opportunity to vote online, they were six to nine percentage points more likely to request a ballot, mobile or otherwise, and three to five percentage points more likely actually to cast a ballot [10]. The research also suggested that approximately half the people casting a ballot with the mobile app would not have otherwise voted if mobile voting was not an option [10]. He estimated that the ability to vote with a mobile device increased turnout by 3-5 percent points [10].

Many people in Prof. Fowler's survey submitted a Federal Post Card Application (FPCA) because they were curious about mobile voting. However, for unknown reasons, they chose not to follow through and cast a vote. [10, p.13]. He also found that the effects of mobile voting on FPCAs and turnout appeared to be larger, especially for women, despite only 38 percent of the sample to be females, and the estimated effects of mobile voting were more elevated among individuals over the age of 50. [10, p.14]. Despite many voters being wary of online and mobile voting, when they do have the opportunity, they seem to take up on the offer, and eligible voters are induced to vote who would not have otherwise cast a ballot [10, p.15].

Lessons learned from the usage of the Votaz app

Before West Virginia's pilot voting program with the use of a mobile device, internet voting had never been attempted in a major U.S. election. At the time of the release of the Votaz app, it proved to be the best alternative to existing problems with our voting process, especially to the voters who lived overseas or did not have timely access to absentee ballots, because it was readily available to eligible voters and was within reach of their fingertips. Voatz app sparked innovation and a solution to either complement or replace existing traditional voting processes. Its claim of using blockchain, biometrics, encryption technologies, and voter-verifiable ballots to secure the voting process and electronic transmissions was unique. Just the thought of being able to vote by sitting on the couch while watching Netflix and drinking coffee was exciting. This promising technology could have been widely used throughout the United States and other nations after raising public confidence in the use of the app and after allowing researchers and analysts to test the app to satisfy the confidentiality, integrity, and accessibility (CIA) triad. However, Voatz's reluctance to reveal its technology, processes, and procedures, has limited researchers from conducting further analysis and study of the underlying technology and software used by the app. Transparency and trust build confidence in technologies, and Voatz seems to lack all these attributes resulting in skepticism of Voatz app's security and cryptographic protocols by the elections security and cybersecurity community.

In 2020, students at the Massachusetts Institute of Technology (MIT) conducted a security analysis of the Voatz app. The MIT students found that the app was prone to any known cyber-attacks and security vulnerabilities existent on Amazon AWS and Microsoft Azure because Voatz's documentation of the West Virginia election indicated that the verifying servers were split equally between Amazon AWS and Microsoft's Azure systems [11, p.10]. They concluded that the app was not secure; adversaries could discover a user's vote and disrupt transmissions. Furthermore, the existing protocol on the Voatz app server, if controlled by adversaries, likely had the full power to observe, alter, and add votes as they pleased [11, p.14]. Despite the apprehension of the usage of the app from the computer security and election security community, the app undoubtedly forces us to think of the potential possibilities and advantages it provides to users who cannot access traditional voting tools or have the option to opt-out of those tools. Any similar app or tools, if used for future elections, should be transparent of their underlying technology, address the CIA triad, and identify and mitigate all possible risks to voter's privacy and vote integrity.

Public opinion about voting technology

In 2018, during an online and telephone interview survey conducted on the topic of voting technology with 1,059 voting-age Americans, researchers found that when asked for accuracy of votes cast, voters exhibited "highest confidence" with paper ballots and "lowest confidence" under online voting [10].

Need for app-based mobile voting

In 2009, the U.S. Congress passed the Military and Overseas Voters Empowerment Act (MOVE), which instructed the Federal Voting Assistance Program (FVAP) that they may run pilot programs to test the ability of new or emerging technology better to serve eligible uniformed members and overseas residing U.S. citizens. Additionally, the act also directed the National Institute of Standards and Technology (NIST) and the U.S. Election Assistance Commission to provide best practices or standards to support the projects, should FVAP choose to run a pilot program [12]. Congress wants U.S. citizens to have access to cast their votes regardless of their location. Tools such as app-based voting complement the existing systems and allow access to individuals who otherwise would not be able to vote or choose to prefer to vote using the digital tools.

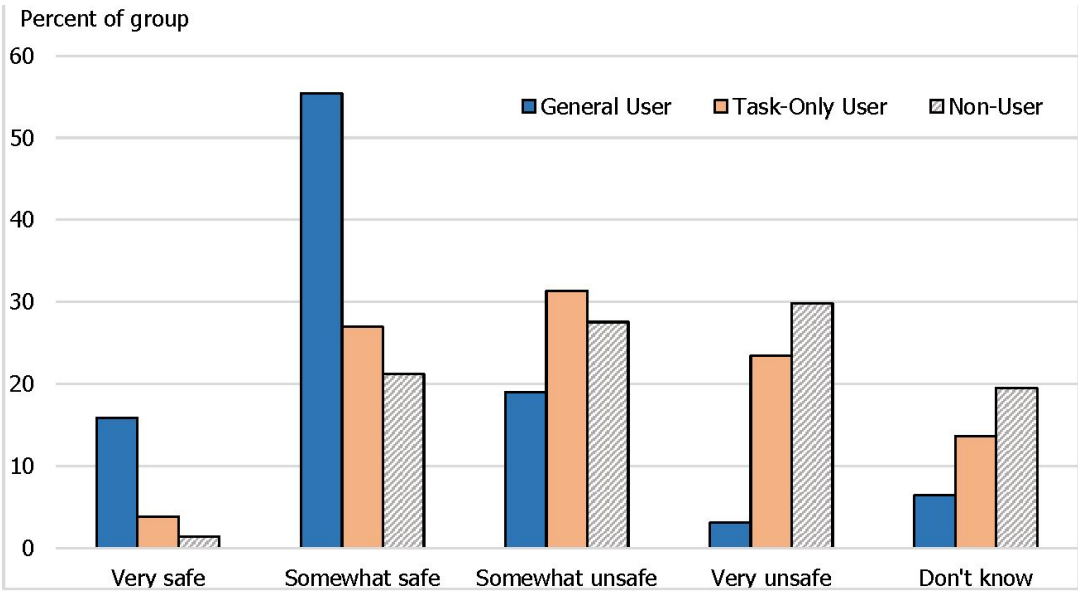
Leveraging a banking app for federal voting

As of June 2019, approximately 96% of Americans now own a cellphone. Furthermore, approximately 81% of Americans owned a smartphone device. This rise was significant compared to 2011, when just 35% of Americans owned a smartphone then. Additionally, of the 81% Americans who owned smartphones, 96%, 92%, and 79% of Americans aged 18-29 years, 30-49 years, and 50-64 years owned a smartphone, respectively. [13, 14]. More Americans, primarily young adults, are more reliant on the use of smartphones for access to online services. It is predicted that the number of smartphone users in the United States will increase to approximately 285.3 million by the year 2023 [15].

Americans have used mobile banking application options since the start of smartphones, and the United States had 57 million mobile banking users in 2019 [16]. In 2017, approximately half of

U.S. adults with bank accounts had used a mobile phone to access a bank account in the past year [17]. While there is a concern of security of personal information of individuals while using mobile banking, surprisingly, a poll conducted by the Federal Reserve Bank on the adoption of and confidence with mobile phone technology, 71% of reported general mobile banking users said their personal information was very safe or somewhat safe using mobile banking [17,18].

Figure 4: Perceived Safety of Personal Information in Mobile Banking



Note: Among U.S. adults with a bank account and mobile phone, percent of each group (general user, task-only user, or not a mobile banking user) [18].

These days, banks are already in compliance with existing federal, state, local laws, regulatory guidelines, and circulars. They also have to follow similar laws and regulations to comply with their e-banking services and their IT infrastructure. Bank Service Company Act, Gramm-Leach Bliley Act, USA Patriot Act, Federal Reserve Bank rules and guidelines, and Federal Deposit Insurance Corporation rules and guidelines are a few examples of laws and controls which govern the banks and their infrastructure. Given that the banks have built their websites and mobile applications to adhere to such strict laws and guidelines, which require a strict standard to protect users' data, finances, personal information, and bank's operations and sensitive information, consumer banking mobile apps could be leveraged to authenticate and confirm the identity of a user and then vector the access to the mobile voting app.

Users' trust on mobile banking

Like any computer device, mobile phones also have their security risks. While the security protocols and crypto technologies used in mobile phones and applications are increasing every year, mobile phone users still seem to be reluctant to trust their mobile phones with their personal information fully. In a 2015 survey conducted by the Federal Reserve of mobile phone users asking them a question "How safe do you believe people's personal information is when

they use mobile banking?", 24% believed that people's personal information was "somewhat unsafe" when using mobile banking, and 18% believed that it was "very unsafe." Only 8% of users found it to be "very safe" to use mobile banking and found their personal information as unsafe [19, p.21]. However, there seems to be a steady rise in the trust of mobile phone users with their personal information over the years. 6%, 7%, and 8% of mobile phone users found their personal information to be safe when using mobile banking for the years 2013, 2014, and 2015 respectively. Furthermore, 32%, 34%, and 35% of mobile phone users found their personal information to be "somewhat safe" while using mobile banking for the years 2013, 2014, and 2015 respectively. The same mobile phone users believed their personal information to be safe when mobile bank [19]. The same survey found that 25% of respondents were concerned with their phones getting hacked or someone intercepting their data [19, p.22].

What minimum information is required to open a U.S. bank account?

In the United States, banks at a minimum require the following information from their customers to open a bank account: Name; Date of Birth; Address; Identification Number (taxpayer identification number, unexpired passport number, unexpired alien identification card number, or the unexpired foreign government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard) [20]. These banks also have procedures put in place wherein they compare the customer data against any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators [20]. While each state traditionally has introduced drivers licenses with their requirement which was not standardized by the federal government, the REAL ID Act of 2005 which is projected to be enforced by 1 October 2020, allows the federal government to set standards for the issuance of sources of identification, such as a driver's license [21]. The REAL ID Act requires, at a minimum, the following documentation: Full Legal Name; Date of Birth; Social Security Number; Two Proofs of Address of Principal Residence; and Lawful Residency Status in the United States [21].

Cybersecurity Challenges and Limitations of Using an App for Mobile Voting

Cybersecurity Challenges: Day after day, mobile applications are susceptible to attacks from both nation-sponsored and non-nation sponsored attackers. A voting app, when created, is undoubtedly to come under attack. Some of the challenges a voting app may face include:

- *Man-in-the-middle (MITM) Attack*: The voting app could be eavesdropped by an attacker where they can intercept a public key message exchange by monitoring and exploiting communication between a server and a client. MITM attackers can bypass single-socket layer (SSL) secure communication maintained by an app by introducing a fraudulent certificate and get secret user information, including their login information (account name and password [22, p.21]. Here if the voting app was to use a temporary session token for access, an attacker could use network sniffing tools to identify the session token for a user and use it to depict the attacker to be the user. MITM attacks could be deterred by using public key pair-based authentication like RSA within the different layers of the stack to maintain encryption and integrity of the communication between the app, the

network, and the final repository server, which would receive all the voter data and vote count.

- *Lack of Binary Protections*: An attacker could reverse engineer the code of the voting app and inject malware and reintroduce and redistribute the app posing a threat. As a result, the app could potentially lose data, which can be avoided by using binary hardening techniques. Furthermore, the voting app should follow secure coding techniques that would detect jailbroken, checksum controls, and debugger detection controls.
- *Insecure Authentication:* User authentication for the voting app is integral to maintain vote integrity. Insecure authentication of a voting app results in weak and vulnerable authentication schemes. An attacker could now use automated, and custom-built attack tools to fake or bypass authentication by submitting service requests to the mobile application's backend server and bypass any direct interaction with the voting app-this process could be easily accomplished via mobile malware within the device or botnets owned by the attacker [23].
- *Weak or Broken Cryptography*: The mobile voting app could be exploited for vulnerabilities and to gain access by attackers if it has weak or bad cryptography or if it is poorly implemented in the app. The attackers can then decrypt the sensitive vote and voter data to its original form and manipulate or steal it. It is recommended that the mobile voting app use the most reliable forms of encryption algorithms from RSA or AES to secure the data and systems.
- *Physical Access*: Physical access and control of the device which has the voting app would stop the individual from voting. If the app is based only on a device, and if the owner of the device had only one device, should the owner not have physical access to the device because they either lost the device or the device was damaged on the day of the voting, they would be unable to vote. Additionally, any person could disrupt the voting process for specific individuals if they remove the physical device away from the individual. The voting app could deter this attack if it could be accessed via not only mobile phones but also through either laptops or other handheld portable devices. The voter could then log into those secondary devices, download the app, and cast their vote.
- *Human Factors:* While attacks by gaining physical access to the device stop the voter from casting their vote, it would be impossible to stop a voter who wittingly allows an attacker access to their device, provides user id and authentication protocols, and wittingly casts a vote preferred to the attacker. If an attacker puts the voter under gunpoint or pressures them to provide them access, the vulnerable voter will have no other means but to allow access. However, security protocols could be built such that the voter is only allowed two tries for authentication to gain access, and on the second wrong try disable voting access to the voter, could potentially deter the unintended vote to be cast. Understandably, no vote is worth a human life, but if such technologies were to be created, and the voters were to be trained on the technology, it could act as a deterrent to voting fraud.

Limitations:

- *Who will create the app***:** There are a handful of federal agencies who could create the app, but the challenge looms of winning the trust of voters who would accept the app and trust its underlying security? Would there be a joint task force created combining solely

of federal agencies to create the app? Or, would there be a USG-Public partnership to ensure transparency of creating such an app?

- *User authentication***:** Users of the app will have to authenticate to gain access to the voting platform. Questions arise of what factor authentication is to be used: single factor, multi-factor, or a one-time token. Multi-factor authentication adds an extra layer of security. However, questions loom on how the voting app users would react to using multiple factors of authentication to gain access to the app.
- *App accessibility*: The app will have to be accessible to all eligible and registered users anytime or during a specified date. Will all users have access to it? How will they gain access to the app? Where will they go to download the app? What would differentiate the app from other apps which are rogue or mimic the original app? Voters such as military members, USG employees, contractors, and civilians who live overseas or in combat zones will need access to the app. How will they download the app and gain access to the app? Furthermore, who will ensure that their voting communication transmission is secure against foreign nation's signals intelligence (SIGINT) collection and sabotage efforts?
- *App usability*: How will a voter know how to download the app? When downloaded, how will they be able to navigate within the app, bypass authentication, and cast their vote? Which agency will provide training on the process of how to use the app? How will the training be delivered? Will it be in-person, online, or via printed material? Will it be in foreign languages to cater to voters who do not speak English or Spanish? Will it comply with the American with Disabilities Act?
- *Vote integrity and voter security*: Once the votes are cast, the votes will need to be verified, locked, and recorded to preserve the integrity of the vote and avoid double voting. How can this be guaranteed? When a member casts their vote using the app, how can the member confirm that their app-ballot was cast and maintain proof that they did vote for a specific candidate or a party? When the vote is cast, how is that specific vote registered and transferred to the office of the election commission overseeing that specific voting? How will the vote, if questioned, be shown that a voter indeed cast that specific ballot and have traceability attributes to the specific user or the device? Moreover, how can transparency of the entire process be guaranteed to the public? Finally, where and how will the data related to the voter and their votes be stored, and which agency or organization will be responsible for maintaining the CIA triad of that data?
- *Voter privacy and vote anonymity:* When a vote is cast, no one but the voter knows whom they voted. The traditional voting methods ensure that the vote's anonymity is ensured. This then maintains the voter's privacy. The voting app which exists so far does not have the security and cryptographic protocols, which can guarantee a voter that their vote's anonymity is intact, and their privacy is ensured. Thus, any app, which, if used for elections, should be able to mitigate these concerns. It should safeguard the voter's privacy while anonymizing their casted vote.
- *Research and development (R&D), and app lifecycle management*: The application will have to undergo plenty of research and development before its release to ensure that it fulfills the CIA triad. It also will need the strictest of authentication protocols and cryptographic algorithms to maintain the security of the app. The lifecycle of the

application would include the planning stage, the technical documentation phase, the prototyping phase, the developmental phase, the quality assurance phase, and the publishing and maintenance phase. The app will also have to ensure that the data is non-repudiated. This is an exhaustive, expensive, and time-consuming process. Who will fund the creation, development, and maintenance of the app and its data? The U.S. Congress may need to introduce and approve a new federal election bill or amend existing laws to earmark funding to fund the R&D and the life cycle management of the federal voting app. They also may need to create new legislation to ensure security and oversight of the voting app.

Recommendations:

- ***Use banking apps for identity verification:*** Banking applications have to maintain specific regulatory and industry-specific standards and have a particular layer of user identity verification protocols established, ensuring only the authorized and verified users have access to the apps. The technology behind such banking apps could then be used to verify the identity of an individual, and then allow the user to gain access to the voting application to supplement the mobile voting app's multi-factor authentication protocols.
- ***Conduct mock trials of voting apps:*** The voting app should go through rigorous stress testing, development, and trials before the release of it to the public. As we have learned from 2020, Iowa State's Democratic Caucus's incident on how an app, if prematurely rolled out for use without proper testing, could catastrophically fail on the implementation day and lose public confidence in the app [9]. The voting app should be beta-tested and tweaked to ensure its flawless execution for the election day.
- ***Train and educate users and public:*** We recommend that members of the public, primarily the voters who opt to use the mobile voting app, receive a significant amount of training on how to download and use the app for its intended purpose. Additionally, to further build public confidence and public trust in the voting app, we recommend that the federal government aid the state and local election officials to provide education to the public on the technology behind the voting app. Furthermore, we recommend that all levels of government, federal, state, and local provide awareness to the public on the validity of the voting app, and on how to download and install an official voting app instead of a malicious voting app.
- ***Introduce more pilot programs throughout the United States:*** We recommend the app to be introduced in small batches in various states like West Virginia and other states, instead of a massive rollout at a national level. Besides, such a step would also help build the public's confidence and trust in the voting app. Furthermore, as more pilot programs are introduced, lessons learned from those programs could be used further to bolster the security and integrity of voting apps. Moreover, the success stories from these pilot programs could be used to garner more "buy-in" from the future voting app users.
- ***Create a public-private partnership:*** We recommend a cooperative arrangement be formed between the U.S. Government and the private industry, with the inclusion of members of the public as an observer of this partnership. This partnership would be solely responsible for the creation, vetting, research and development, security, and roll out of the voting app. They would be entrusted for a "cradle-to-grave" system of the app. It would also ensure that the voter's privacy and their vote's integrity is safeguarded. We

recommend such partnerships to build public confidence and ensure the transparency of the voting app. An example of a public-private partnership is the nonprofit named InfraGard, a partnership between the Federal Bureau of Investigation (FBI) and the private sector that protects U.S. critical infrastructure and the American people. They educate, train, and share information amongst private industry members, who primarily represent critical infrastructure sectors. Several success stories of the group include incidents when the private industry shared valuable information to the FBI, regarding banking fraud involving large sums of money, defacement of state agency websites due to a computer intrusion, and a SQL injection attack which malicious inserted codes into a company's website, enabling attackers to gain customer's orders and credit card information, benefitting investigations of the FBI [24].

- ***Introduce the app as an opt-in alternative to the paper ballot:*** As public opinion has shown that voters exhibit the highest confidence with a paper ballot and lowest confidence under online voting [10], we recommend the voting app be introduced as an option to the paper ballot and absentee ballots. We are optimistic that this approach would be more acceptable to voters.
- ***Conduct more research:*** App-based voting technology remains new and unventured. It lacks extensive research and testing data to prove its usability and provide confidence in its security and app integrity. We recommend the introduction of more research grants from the federal government and the private industry to the computer science and cybersecurity community to conduct further research on the feasibility study of the mass use of apps for elections.

Conclusion

The idea of using a mobile application for voting is promising. With the increase of global access to smartphones, we will continue to see a rise in users' confidence and dependence on apps, and we believe voters will welcome and accept a voting app. The public is still yet to place their highest level of confidence in sending personal information on a mobile application. However, if a public-private partnership entity would create a secure voting app and provide oversight on its testing and deployment, the public's confidence and trust in the app could significantly increase. Also, it is important to provide proper education and training of the app to the public and the app users.

A voting app could increase voter turnout and help combat voter fraud. Also, a voting app could aid the Uniformed and Overseas Citizens Absentee Voting Act, effectively utilizing the Technology Pilot Program as listed under 42 USC 1973ff-7, SEC. 589, and help establish an electronic medium for eligible U.S. citizens and uniformed members to cast their votes timely and globally.

Today, we, as a nation, are not ready to fully utilize a voting app in place of traditional voting methods. However, as we conduct more research and testing on voting app integrity and security, voting apps could be gradually introduced as pilot programs throughout the United States and eventually broadly deployed as an effective alternative to traditional voting methods.

References

[1] A. Gumbel, Election Fraud and the Myths of American Democracy, Social Research, vol. 75, no. 4, pp. 1109-1134, 2008. Available: JSTOR, https://www.jstor.org/stable/pdf/40972109.pdf [Accessed Sept. 3, 2019].

[2] www.whitehouse.gov. (2019). The Heritage Foundation, A sampling of election fraud cases from across the country. [Online] Available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/docs/pacei-voterfraudcases.pdf [Accessed Sept. 3, 2019].

[3] F. Lynn, "Boss tweed is gone, but not his vote," The New York Times, 09-Sep-1984. [Online]. Available: https://www.nytimes.com/1984/09/09/weekinreview/boss-tweed-is-gone-but-not-his-vote.html [Accessed: Sept. 3, 2019].

[4] Findlaw. (2019). FindLaw's Court of Criminal Appeals of Alabama case and opinions. [Online] Available at: https://caselaw.findlaw.com/al-court-of-criminal-appeals/1091907.html [Accessed Sept. 3, 2019].

[5] Findlaw. (2019). FindLaw's Court of Criminal Appeals of Alabama case and opinions. [Online] Available at: https://caselaw.findlaw.com/al-court-of-criminal-appeals/1091907.html [Accessed Sept. 3, 2019].

[6] www.sos.wv.gov. (2019). WV Secretary of State. [Online] Available at: https://sos.wv.gov/elections/Pages/MobileVote.aspx [Accessed Sept. 27, 2019].

[7] B. Freed, R. Johnston, and C. Wood (2019). West Virginia says it wants to do more mobile voting | StateScoop. [Online] StateScoop. Available at: https://statescoop.com/west-virginia-says-144-people-voted-using-mobile-blockchain-app/ [Accessed Sept. 27, 2019].

[8] L. Mearian (2019). Utah County to pilot blockchain-based mobile voting. [Online] Computerworld. Available at: https://www.computerworld.com/article/3410570/utah-county-to-pilot-blockchain-based-mobile-voting.html [Accessed Sept. 19, 2019].

[9] A. Schneider, "What We Know About The App That Delayed Iowa's Caucus Results," What We Know About The App That Delayed Iowa's Caucus Results, 04-Feb-2020. [Online]. Available:https://www.npr.org/2020/02/04/802583844/what-we-know-about-the-app-that-delayed-iowas-caucus-results [Accessed Mar. 20, 2020].

[10] A. Fowler, "The Promises and Perils of Mobile Voting" in Election Sciences, Reform, & Administration Conference (ESRA), Philadelphia, PA, 2019, pp. 1-27. [Online]. Available at

https://drive.google.com/file/d/1aKVRaWY_Stzr1ba7feXYCv8KHRaRkA-0/view [Accessed Sept. 3, 2019].

[11] M. Specter, J. Koppel, and D. Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections, pp. 1-14 [Online]. Available: https://internetpolicy.mit.edu/securityanalysisofvoatz_public/ [Accessed Mar. 20, 2020].

[12] United States Government, 'National Defense Authorization Act', 2010.

[13]"Mobile Banking: Rewards and risks," Federal Deposit Insurance Corporation. 19-Dec-2011 [Online]. Available: https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.html [Accessed Nov. 1, 2019].

[14] "Figure: Mobile Application Security by Type of Application, Mobile Banking: Rewards and risks," Federal Deposit Insurance Corporation. 19-Dec-2011 [Online]. Available: https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.html [Accessed Nov. 1, 2019].

[15] A. Holst, "Number of smartphone users in the U.S. 2010-2023," Statista, 30-Aug-2019. [Online]. Available: https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/ [Accessed Dec. 10, 2019].

[16] M. Szmigiera, "Mobile banking in the U.S.," www.statista.com., 08-Oct-2019. [Online]. Available: https://www.statista.com/topics/2614/mobile-banking/ [Accessed Dec. 10, 2019].

[17] E. A. Merry, "FEDS Notes," The Fed - Mobile Banking: A Closer Look at Survey Measures, 27-Mar-2018. [Online]. Available: https://www.federalreserve.gov/econres/notes/feds-notes/mobile-banking-a-closer-look-at-survey-measures-20180327.htm [Accessed Dec. 10, 2019].

[18] E. A. Merry, "Figure 4: Perceived Safety of Personal Information in Mobile Banking, FEDS Notes," The Fed - Mobile Banking: A Closer Look at Survey Measures, 27-Mar-2018. [Online]. Available: https://www.federalreserve.gov/econres/notes/feds-notes/mobile-banking-a-closer-look-at-survey-measures-20180327.htm [Accessed Dec. 10, 2019].

[19] Board of Governors of the Federal Reserve System, "Perceptions of Safety and Risks" in Consumers and Mobile Financial Services 2016, Mar-2016, pp. 1-27. [Online]. Available: https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf [Accessed Dec. 10, 2019].

[20] “FDIC Law, Regulations, Related Acts - Miscellaneous Statutes and Regulations,” Federal Deposit Insurance Corporation, 31-Aug-2017. [Online]. Available: https://www.fdic.gov/regulations/laws/rules/8000-1600.html [Accessed Dec. 10, 2019].

[21] “REAL ID Frequently Asked Questions,” Department of Homeland Security, 19-Dec-2019. [Online]. Available: https://www.dhs.gov/real-id-frequently-asked-questions [Accessed Dec. 10, 2019].

[22] Linxi Zhang, “Experiment Implementation” in Smartphone App Security: Vulnerabilities and Implementations, M.S. thesis, Univ. of Michigan-Dearborn 2018, pp. 1-51. [Online]. Available: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/143522/Linxi-thesis-submission.pdf [Accessed Dec. 20, 2019].

[23] “M4: Insecure Authentication,” OWASP. [Online]. Available: https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication [Accessed Mar. 20, 2019].

[24] “InfraGard: A Partnership That Works,” FBI-InfraGard: A Partnership That Works, 08-Mar-2010. [Online]. Available:https://archives.fbi.gov/archives/news/stories/2010/march/infragard_030810 [Accessed Apr. 16, 2020].