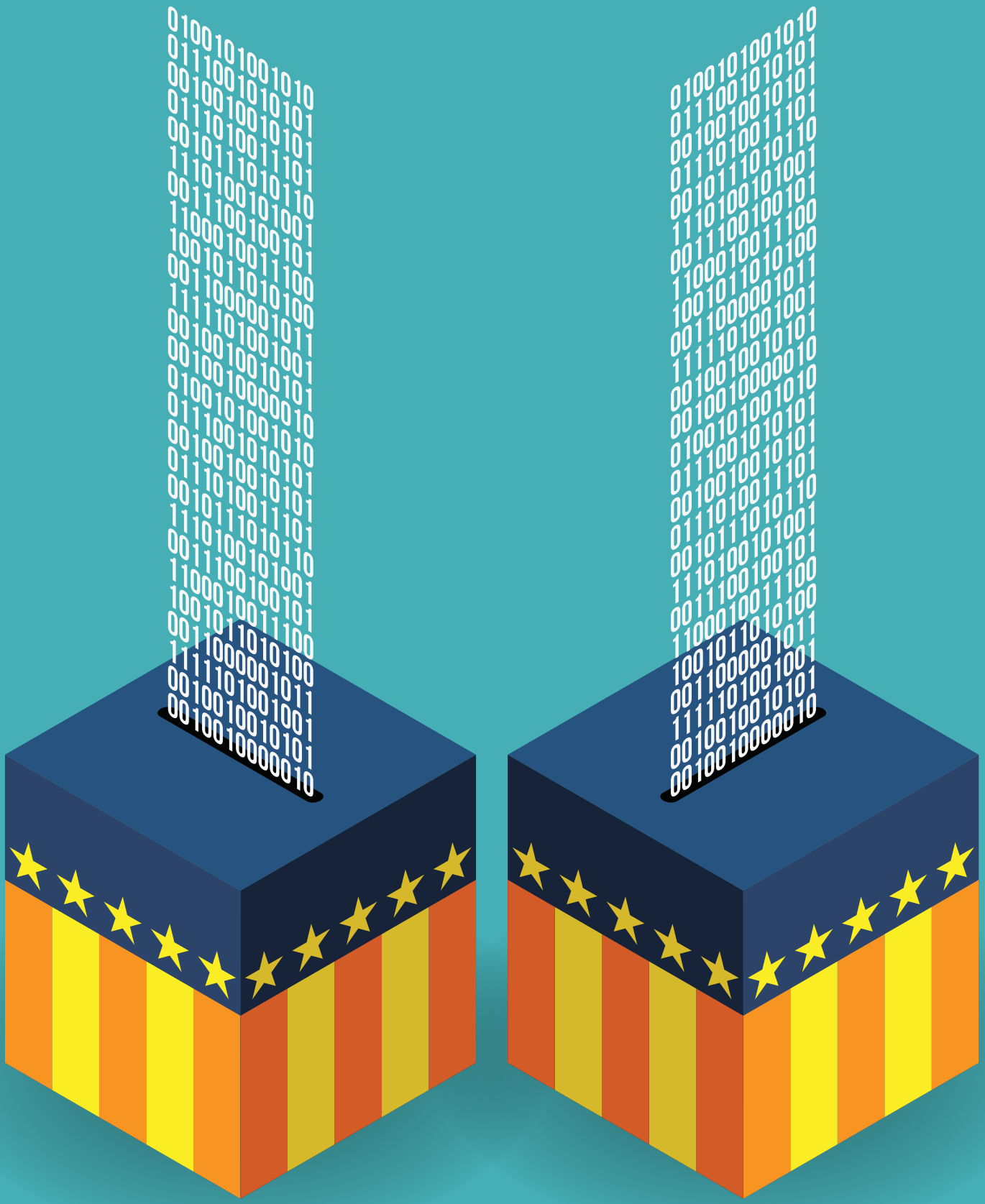

Making Voting Easier for Disabled and Overseas Voters:

Secure, Accessible Virtual Voting Infrastructure

Ted Selker and **Justin Pelletier,** Rochester Institute of Technology

Insights

- To ensure trust in the process, all of the many aspects of voting need to be supervised.
- Human oversight of disabled and overseas voters can not only help with authentication but also ensure overall voting success.
- SAVVI demonstrates how carefully curated electronic ballots can be an improvement over absentee ballots for disabled and overseas voters.

IMAGE BY HERMIN / SHUTTERSTOCK.COM

The user experience of voting seems simple: a mark next to a choice. The fact that it determines the direction society is headed makes creating and counting this mark a central point of control. Organizing voting processes to collect, count, and report votes correctly often seems like an arms race between major political players. Indeed, people serve time for felonies, including stopping voters from getting to a polling place, turning them away, giving them incorrect ballots, destroying or subverting the mechanisms for depositing votes, not depositing ballots, destroying deposited ballots, altering ballots, and incorrectly counting ballots.

Civilization learned a millennia ago that, without privacy at a polling place, a bystander could see a voter putting an ostraca (a shard of pottery) in a vessel for a particular candidate. Since then, there have been many attempts to instill trust by ensuring voting privacy and integrity. The secret ballot, for instance, was a significant step toward this goal; adopted in 1856 in Australia, it was a way of allowing citizens to vote without recrimination. The U.S. was slower to protect anonymity. In 1869, Thomas Edison's electric voting machine was rejected, as it would have allowed members of Congress to vote in private; constituents wanted to know that their representatives were representing their wishes. It took until the 1890s for the U.S. government, responding to widespread concerns about voter intimidation and influence,

to adopt the secret ballot. Some also promoted it cynically because it disallowed help for illiterate and disabled people to cast a ballot, suppressing these vulnerable people's participation. Some countries have not gotten there yet, expecting voters to put a preprinted ballot in a ballot box in clear view of others, which does not prioritize privacy.

Secret ballots for private voting have included both untraceable, ballotless voting options using levers and direct-recording electronic voting machines and ballots that might be audited. Mark-sense ballots that showed selectable choices that could be easily audited and punch cards that weren't easily auditable both debuted in the early 1960s.

For most of the past century, voting outside of a ballot booth was the highest source of fraud in the U.S. election system [1]. In spite of this, many states embrace mail-in ballots, claiming they're both convenient and auditable. For example, during the Covid-19 pandemic, mail-in voting became a popular way for vulnerable people to vote safely. Still, some mail-in ballots never reach the voter or are lost or spoiled by the voter. Some ballots are filled out by family, friends, or acquaintances of the voter, which is a felony. Some ballots are not returned in time to be counted or are sent to the wrong address, or the envelope is used incorrectly. Various other small but consequential problems stop ballots from being included in the vote. There are even more challenges for disabled voters—for some people, marking a paper ballot, putting it in the envelope, and mailing it without assistance can be impossible.

Auditing mail-in ballots is also problematic; new paper ballots are "found" and added to recounts, hand recounts don't give repeatable results, and selections on ballots sometimes get changed [1]. As well as compromising privacy, mail-in ballots for some classes of voters have additional problems [1,2]. Overseas American voters have had difficulties getting mail-in ballots to their home polling places. Blind voters and people with limited manipulation skills are unable to use a mail-in ballot privately and independently. For these voters, some states, including North Carolina and Massachusetts, have allowed ballots to be delivered, marked, and returned electronically.

To address some of these issues and thereby advance voting technology and accessibility, we sought to describe a system that eliminates an expensive procurement process, reduces the need for new software, and avoids using security approaches that require deep expertise.

In so doing, we aim to integrate confidentiality, integrity, and availability for disabled and overseas voters. Confidentiality demands independent marking, submission, and protecting ballots in transit and counting. Integrity requires that votes are cast and counted as intended. In several important ways, accessibility is synonymous with availability for disabled and overseas voters.

OVERSEAS AND DISABLED VOTERS

Even with the support of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), some 3 million *overseas voters* still experience pernicious ballot delivery delays. In 2006, only 26.5 percent of those requesting a ballot succeeded at having it counted. Even if they are allowed to e-vote, they might miss the emails, have trouble with software, or not return the ballot correctly. Security issues have also been a major concern.

Disabled voters continue to find accommodations inadequate and vote in much fewer numbers than other voters. Section 508 of the Rehabilitation Act defines functional requirements for technologies that accommodate nine classes of Americans with vision, speech, hearing, physical, and seizure disabilities.

Voters with no or limited vision have used magnifiers or audio to vote. We know of no workable prosthetic for allowing blind people to privately and independently vote on mail-in ballots. Braille may seem appropriate, but only some 10 percent of blind voters use braille.

Deaf and mute voters also face challenges with most conventional voting technologies. More than 14 percent of these voters have reading disabilities and more than 6 percent have some short-term memory problems. Structuring ballots for deaf and mute voters can greatly reduce their errors [4]. Filling out and bringing a sample ballot as a memory aid universally reduces voting errors.

Polling places need to continue to work at making themselves accessible to people with mobility problems. Manipulation problems require accessibility technology such as large buttons, mouth sticks to press buttons, or vote-marking machines equipped with ways of making selections by sucking or blowing using so-called sip-and-puff technology.

By letting voters know their vote is included in the count, new verification approaches give much-needed evidence to increase confidence in outcomes.

Projects such as Remotegrity and VoteXX have special security features but also notoriously complex user experiences that do not address independent, private voting for people with disabilities.

USABLE SECURITY IN ELECTRONIC VOTING

Concerns about electronic fraud have affected the way we think about elections. Misinformation campaigns, such as foreign messaging in the 2016 presidential election, are common for reducing voter turnout. In some countries, armed actors stuff or steal ballot boxes. Will bad actors turn from misinformation to attacking voting systems in the U.S. too? And how will these threats affect disabled voters?

The disabled community has had low voting turnout historically; weak security for them could still lead to flawed elections. Layering best-practice protections can improve security and access. Addressing their needs for confidentiality, integrity, and availability could also solve problems for other types of voters. The Federal Election Commission and the Election Assistance Commission (EAC) have created voting-system certification recommendations to minimize risks. Most states follow the EAC's Voluntary Voting Systems Guidelines (VVSG) for voting systems and follow guidelines for testing and scrutiny defined by the National Institute of Standards and Technology.

Missing from the VVSG, however, is a secure way of transmitting electronic votes. To address this, we constructed an architecture that can balance accessibility, confidentiality, and integrity for remote voters while minimizing the burdens to the voter and election boards.

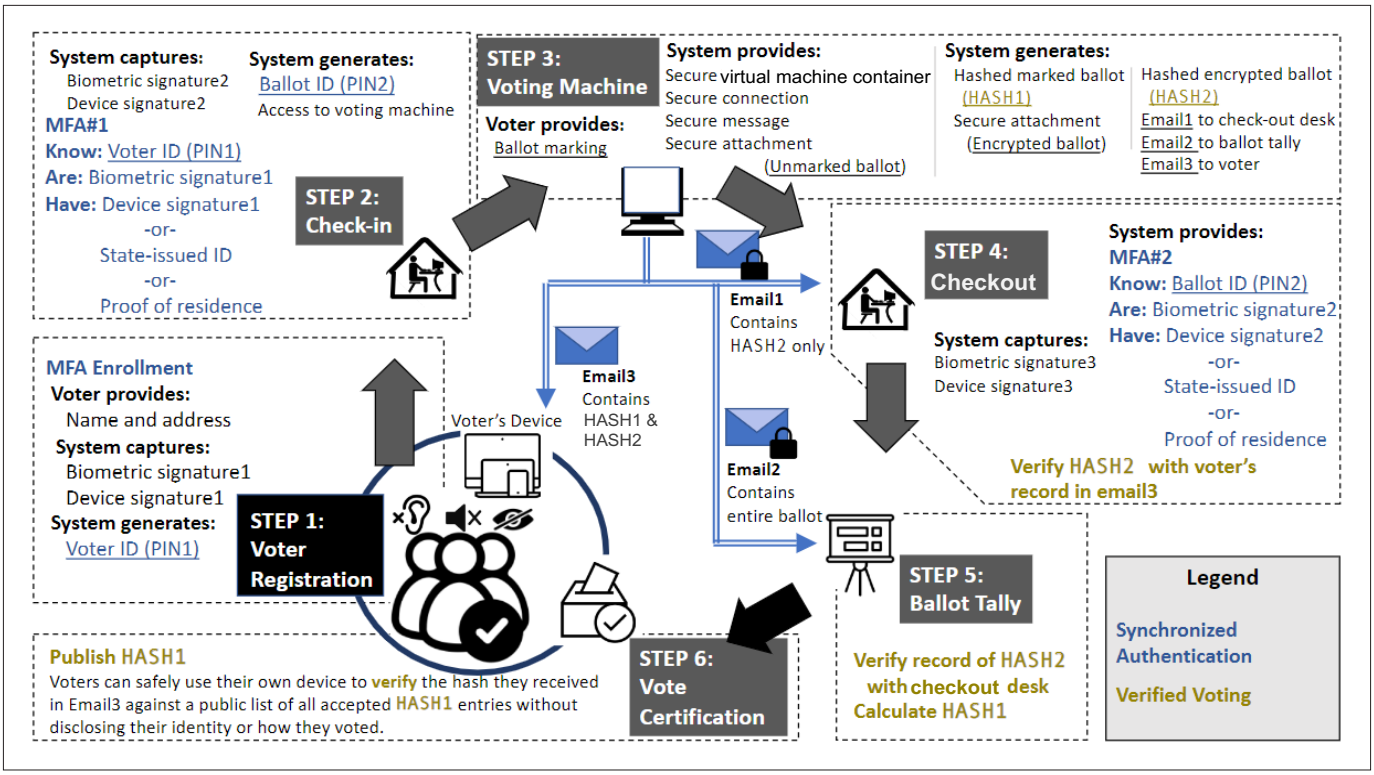

Figure 1. The six steps of creating an easy-to-implement, credible voting system for people who can't vote in person at their polling place: the secure, accessible virtual voting infrastructure (SAVVI).

PROPOSING A SECURE, ACCESSIBLE VIRTUAL VOTING INFRASTRUCTURE

In the run-up to the 2020 presidential election, most people were concerned with blunting the pandemic by avoiding respiratory exposure to others. In exploring inexpensive methods of giving people with disabilities a way to vote that was less prone to interference, we looked at possibilities for improving the confidentiality, integrity, and accessibility for UOCAVA voters too. The secure, accessible virtual voting infrastructure (SAVVI) was the result of responding to election officials' challenges. The SAVVI system addresses security as a usability problem [5], automating processes to encrypt emails and their contents and to better secure containers that allow remote ballot marking and submission.

We focused on the following requirements:

• *Prove to voters that their vote was cast as intended and recorded as cast.* Giving voters a way to see that their selections were tallied should increase trust in the electoral process.

• *Be resilient to technology change.* The infrastructure should incorporate best-in-class security as it becomes available.

• *Allow remote voting from personal devices.* Use devices familiar to voters with access technology implementations.

• *Leverage process familiarity.* Copy in-person voting steps for trust and security purposes, including checking in with a person at both the beginning and end of each voting experience.

SAVVI DESIGN

The design process began with an analysis of concerns about using private computers for voting. We then considered what can be done to address these concerns for disabled or UOCAVA voters. We proposed using multiple layers of security in a coordinated way (i.e., defense in depth) with synchronized multifactor authentication and ballot-integrity verification using commercial off-the-shelf security techniques in a six-step protocol (Figure 1).

Step 1: Voter registration. We start with the popular security concept known as multifactor authentication (MFA). MFA works with more than one of the following security factors: something you have, something you know, and/or something you are. The voter registration identification number (PIN1) is *something you have* that comes separately through the U.S. Postal Service. The voter uses the PIN1 in the check-in process. The *something you have* factor could be a signature of the device to augment multifactor authentication. *Something you are* starts with a test of "humanness," such as completing a captcha perceptual recognition puzzle. This can be furthered with a voter's voice audio or a video of their face stating, for example, their name, address, and phone number. To reduce fraud, such an authentication should be interactive, as it is in a polling place with humans at a check-in desk.

Step 2: Check-in. Checking in with a human verifier can help overcome the confusion of getting ready to vote and will test humanness at a virtual check-in desk. As at polling places, this can be a powerful MFA tool in authorizing remote voting.

Once the voter is authenticated, the check-in desk sets up a virtual container with access to voting and authorizes a specific private voting device and path to it. Check-in establishes a secure connection with a ballot identification number (PIN2) that allows them to authenticate with the voting machine itself.

Step 3: Accessing a voting machine. The system sets up a unique virtual voting machine for each voter. This separates personal registration information and confirmation from private voting data. The process involves

the following key elements:

• *Virtual voting machine (VVM):* A 2018 National Academies report reminds us that a system can be corrupted at any layer. SAVVI adds protection against this with its dynamic provisioning of a VVM at voter check-in, and retires that machine upon checkout. This adds difficulty for any software trying to change a vote by accessing the voters' device. Home voters will use different systems on different networks to access the secured VVM within a secured channel, which will make any hacking attempt through the voters' personal devices much harder to scale.

Off-the-shelf software is available to create these VVMs and secure them. A "virtual container" lets each voting machine be built in real time through tools like Docker, Terraform, and Ansible. This simplifies the verification of system security and usability at the check-in desk. The short life cycle of each machine also presents a reduced attack surface because hackers will have less time to compromise a voting device. The voter can be required to access the VVM through a secure tunnel across the Internet; such virtual private network support and secure connection using a transport-layer tunnel are available within popular Web browsers.

• *Secure connection:* On their secured machine, a voter chooses between secured ballot-return options like secured versions of email services and browsers they are used to. A browser-based email service can enforce Advanced Encryption Standard (AES) and Transport Layer Security (TLS) 1.3 to prevent eavesdropping, tampering, and message forgery. TLS 1.3 uses public-key encryption to secure websites and browser-based email. Ongoing improvements to protocols such as TLS are best-in-class technologies that keep the browser-based email service running on the VVM to remain up to date.

• *Secure message:* Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME) have added a layer of security to the message itself and are widely used. Today's S/MIME 4.0 works with Gmail, Outlook, and other email systems. It provides digital signature for authentication and integrity and validates that email was sent by the user.

• *Secure attachment:* Preloaded scripts hash and then encrypt the ballot; hashes to the encrypted ballot again will supplement voting integrity.

Hashing uses a code to map and encode data into a standard-length string. It can be used to check whether the contents of a message have been altered. We recommend 512-bit hashing (SHA-512), which is double the U.S. federal standard and essentially free to use because it's built into most computer systems. SAVVI sends a copy of the hashed ballot as well as the hash of the encrypted ballot to the checkout desk and to the voter. This gives transparency to both the checkout desk and voter. Importantly, it allows voters to verify that their electronic ballot was recorded as cast and ultimately allows distributed verification that the election was tallied as intended.

Encryption is constantly improving, and open-source audited encryption software solutions have been shown to be less vulnerable than hardware-based encryption. As of early 2021, one exemplar, VeraCrypt, offered five encryption algorithms, each with a minimum practical security of 100 bits, and 10 multilayer encryption combinations called cipher cascades. Many other encryption suites exist. The VVM can use simple scripts to create cipher cascades to protect the ballot itself.

Step 4: Checkout. Vote logging checks the voter's receipt (of the hash of their encrypted ballot with the desk's receipt of that hash) at the virtual checkout desk. As with the check-in desk, this signature should be verified using an interactive voice or image excerpt from the live phone or video feed with the checkout desk.

Step 5: Vote tally. The record is verified through hashing with the checkout desk, which then routes the encrypted ballot for decryption and calculates the hash of the plaintext marked ballot for vote certification. A simple website can list the hash of each tally without revealing who cast the vote or how they voted, which allows voters to verify that their vote was counted.

Step 6: Vote certification. Once their ballot has been decrypted and tallied, a voter gets a certification confirming their ballot has been counted, along with the public, anonymous hash. Even a small number of voters' matching hashes on a public website has been shown to help assure election integrity.

SECURITY CONSIDERATIONS

To analyze the security of SAVVI, we consider five realistic and high-impact attack models:

• *Denial of service (DOS).* Overloaded voting systems are a particular concern when everyone votes on Election Day. DOS attacks have become less feasible, with much of the country getting ballots up to 60 days before Election Day. In any case, SAVVI's email server can defeat a flood of illegitimate email by white-listing emails from the VVM. Once the ballot is cast and the voter checks out, the email server removes the entry.

• *Spoofing.* Attackers might present someone else's credentials. The phone calls, one at voter registration and another at ballot deposit, establish humanness and defends against spoofing. The system might further recognize and direct fraudulent voice prints to a "honeypot," which allows the attacker to demonstrate their nefarious goals while not affecting the election. We have tested this automated setup for finding and catching would-be election system attackers [6].

• *Phishing.* Malicious links or attachments in an email might be used to steal a person's credentials or compromise their device. SAVVI's unique voting email is available only through a secure virtual container once the voter verifies with an election official for one-time use. Even if an attacker guessed all potential email addresses and sprayed phishing emails across them, the secure virtual container could purge the emails upon loading the email client.

• *Shoulder surfing.* A person physically colocated with the voter could view or coerce actions. The check-in process helps stop this by explicitly requiring affirmation that the voter is alone and voting privately.

By securing the remote voting process for disabled and overseas voters, we can establish superior options for all voters.

• *Person-in-the-middle.* Person-in-the-middle and eavesdropping are potential threats in Internet communications. Three layers guard against this: 1) the process of validating a voter, 2) giving voters a new email address with each virtual voting machine to send their vote from, and 3) using secure virtual containers, which automate the encryption of the webmail channel, the marked ballot, and the email message itself (S/MIME).

CONCLUSION

Many transactions like banking can be verified later with the legitimate user sharing who they are. Not so with voting, because our society prioritizes anonymity in how a person votes; the added difficulty of protecting privacy while establishing accuracy and integrity makes electronic voting a security challenge. Configuring a SAVVI system with off-the-shelf tools overcomes many of the problems of electronic voting. We show how available security techniques, with multiple layers of security and human supervision, can be used to overcome many challenges for overseas and disabled voters. This will reduce or eliminate the need to send ballots by unsecured email or to fill out paper ballots through intermediaries. The approach can also empower physically disabled people to vote independently.

SAVVI uses human-in-the-loop and available technology to reduce opportunities for coercion, vote selling, and voting machine hacking. It can improve user experience and secure voting that can be implemented by a voting jurisdiction with their IT professionals. AES, TLS, and S/MIME represent available and open source components that can work together to protect information in transit. SAVVI automates the preparation and orchestration of these tools to provide increased usability and security.

Detecting intrusion attempts before they cause harm is preferable to having to mitigate the harm after it is done. In other work, we have shown that honeypot voting systems can discover and entrap the attempts of hackers seeking to compromise voting systems [6]. Including humans at check-in and when the vote is deposited offers huge improvements through multifactor authentication security. The human check-in also gives important support to the setup and successful completion of voting; it should also aid adoption by providing voters with a process they're used to in physical polling places.

One piece of software or one person alone should not be able to register voters; make or control the data of registered voters; design, print, or handle ballots; set up a polling place; open a poll or polling place; check in a voter; provide a ballot; turn away a voter; log onto voting servers; make changes to voting servers; work with ballots or voting records; log votes and count ballots; certify voting counts; or report voting counts. Each of these steps requires supervision to ensure elections are trustworthy. We have personally seen this principle ignored, and in each case it has yielded problems. This concept includes the need for the oversight of software and humans, a singularly powerful way of avoiding any one problem causing voting system mistakes and malfeasance. These redundant controls make every link in the chain stronger.

For a democracy to work, it is essential that every registered voter can get, fill out, and return their selections. We must catch errors in ballot design, layout, printing, delivery, depositing, storing, counting, and reporting. We must also include auditing approaches that proactively find and reduce errors. Voters must have a way to verify that their vote was properly counted. SAVVI shows a way that disabled and overseas voters can succeed at voting independently and privately, using inexpensive and widely available technology

The SAVVI process shows how user scenarios can improve security—even in contested elections. We think that the user interface community could help improve most security applications. We hope that SAVVI shows how a highly complex and technical scenario can be improved through user experience design. As is true with most accessible technologies, we believe that creating solutions for people with disabilities can help solve other users' problems as well. By securing the remote voting process for disabled and overseas voters, we can establish superior options for all voters. In this, we may well have taken the first step toward a more trustworthy democracy.

ACKNOWLEDGMENTS

This research was funded in part by the Eaton Cybersecurity SAFE Lab at the Rochester Institute of Technology. We would like to thank the attorneys at Brown, Goldstein, and Levy for encouraging this work. Justin Pelletier would also like to acknowledge the support he receives from *Ordo Praedicatorum*.

ENDNOTES

1. Ansolabehere, S. and Stewart III, C. Residual votes attributable to technology. *The Journal of Politics 67*, 2 (2005), 365–389.
2. Voting Technology Project. *Voting: What Is, What Could Be*. Caltech/MIT Voting Technology Project, 2001.
3. Banel, F. Memories still raw for candidates from 2004 race for Washington governor. MyNorthwest. Nov. 5, 2020; https://mynorthwest.com/2289152/memories-still-raw-for-candidates-from-2004-race-for-washington-governor/
4. Selker, T. The technology of access: Allowing people of age to vote for themselves. *McGeorge Law Review 38*, 4 (2016).
5. Selker, T. and Pelletier, J. Secure, accessible, virtual voting infrastructure (SAVVI): Reducing barriers for disabled and overseas voters. *Proc. of 46th MIPRO ICT and Electronics Convention*. IEEE, 2023, 1230–1239.
6. Madden, M., Szafaran, D., Gray, P., Pelletier, J., and Selker, T. A canary in the voting booth: Attacks on a virtual voting machine. *Proc. of International Conference on Digital Forensics and Cyber Crime*. Springer, Cham, Switzerland, 2024, 3–18.

Ted Selker is codirector of the Caltech/MIT Voting Technology Project and founder of Carnegie Mellon University's (CMU's) Research on Accessible Voting. He has researched voting technology since 2000 and is currently at the Rochester Institute of Technology. He was a professor at CMU Silicon Valley for five years and at the MIT Media Lab for 10 years. Selker is known for his work as an IBM Fellow. His considerate systems inventions and research focus on using cognitive science in the service of people.
→ Ted.selker@gmail.com

Justin Pelletier is director of the Cyber Range at the Rochester Institute of Technology. He is founding director of the National Security Agency–funded National Consortium for Cyber Governance, Risk, and Compliance. He has also worked as a member of the U.S. National Security Council modeling and simulations working group.
→ jxpics@rit.edu

DOI: 10.1145/3688156