Neuvote

WHITE PAPER

THE HYBRID MOBILE VOTING SYSTEM™

WHY NEUVOTE'S HYBRID METHOD SATISFIES ALL 5 BARRIERS TO MOBILE VOTING

INTENDED AUDIENCE: ELECTORAL ADMINISTRATORS

AUTHOR: MATTHEW HEUMAN
MARCH 2019

Contents:

A MESSAGE FROM NEUVOTE:

Whether an online voting system can be truly secure has been thoroughly debated for the past 30 years. Systems have been developed and case studies have been examined but unsurprisingly with an institution as important as our democratic electoral process, no general consensus has been reached regarding how online voting systems can be implemented that equals the overall integrity of the paper ballot voting system.

Any proposed solution should start with replicating this integrity as its foundation rather than treating the voting process as a problem that can be solved with software alone.

The following white paper from Neuvote took the traditional voting process and determined that it didn't need to be revolutionized to work. The principals off the process were as effective now as they were in 139BC, it is the accessibility of those services that was no longer copacetic with contemporary voters. To create a functional online voting system required looking at augmenting the traditional voting model with advances in communication technology rather than overhauling the entirety of the system as a whole.

Neuvote's proprietary system is a hybrid model build for mobile use only because not only do smartphones have added security benefits, but they also are the primary method that people access the internet and each other.

The following sections will outline the field of online voting, the barriers prohibiting adoption and how the Neuvote system overcomes those barriers by augmenting the traditional model with innovative digital solutions.

EXECUTIVE SUMMARY:

The fierce debate surrounding online voting stems from the strong emotional attachment people have to the political process. These emotions are compounded by the difficulties online voting have in addressing the fundamental concerns around the digitalization of democracy. People have a vested interest in ensuring that any attempt to move elections online are treated with the utmost respect for the traditional process.

One of the main issues with traditional method of voting and one that online voting has the potential to address, is increased voter accessibility. Modern life and how people interact and connect to the world at large is no longer in sync with the traditional voting requirement of going to a polling location. The way people consume information and interact with services has changed dramatically and the electoral process has not kept up with these changes resulting in low voter engagement.

Other benefits online voting can offer include: greater privacy, youth engagement, reduction in ballot errors, and expedited tabulation and improved accountability. These benefits have the capability to greatly enhance the democratic process by increasing the efficiency and engagement of an election.

There have been numerous technologies proposed to facilitate the transfer of a vote via the internet in a safe and secure method but none have managed to be adopted successfully on a large scale in a high level election because of these fundamental barriers:

1. Data Security
2. Authentication
3. Confirmation
4. Privacy & The Secret Ballot
5. Verifiability / Auditability

If trust is to be established in an online voting system, these barriers must be satisfied completely.

Voters, election administrators and politicians must trust in the system because without the same standard of trust that voters have in the traditional method, an online voting system will never be able to be fully implemented successfully.

Representative democracy is based on the principle that we elect an individual to be the people's voice in government. If the system used to elect those representatives is not trusted to be secure in its method then the entirety of the system is called in question.

COLD WALLET, HOT WALLET AND MONEY UNDER THE MATTRESS

Blockchain backed crypto currencies are hypothesized as a decentralized answer to modern banking. They allow users to "mine" coins using sophisticated algorithms to produce the virtual currency that can be exchanged publically across a network. These coins are typically stored in a virtual wallet either on an online exchange or on an individual's personal computer.

Regarding security in the crypto market, the current methodology is to store the coins offline in a "cold wallet" that is not available to intrusion. Storing the coins on an exchange or on a PC that is connected to the internet is considered a "hot wallet", meaning a hacker can access the wallet and transfer the coins to another location which has been done many times in the crypto markets short history.

The "cold wallet" method is typically a USB drive or external hard drive that is disconnected from the network. This method is a good example of an analog process augmenting the fully digital service for advanced security. The only problem that exists with this augmentation revolves around keeping that external source safe. If

the USB or external drive is lost or corrupted the coins are equally lost, a tenet that was famously brought to light when a man accidentally threw away an old hard drive with essentially millions of dollars in Bitcoin stored on it.

For people apprehensive with keeping their money in a bank, the old adage of storing it under a mattress was a way to verify your funds tangibly, albeit not very secure. The mattress was not connected to any network but was severely exposed if anyone were to come upon it. The concept of a cold wallet in crypto currency is essentially the same as storing your money under a mattress except when it comes to digital denominations, you can't see, feel or confirm that the money is still there in the same way you can by simply lifting up the bed.

These examples are a good equivalent to the concept proposed in this white paper. Keeping a vote stored digitally has the same security as the crypto wallets. The hot wallets are vulnerable to manipulation due to their connectivity but even the cold wallets are vulnerable to something as simple as a strong magnet.

Storing money under a mattress comes with its own set of security issues but at least barring theft or the place burning down, can generally be used to visually confirm that all the physical funds are there.

Using a hybrid model that features analog and digital data security backed with visual confirmation allows a vote to be transferred from a user's device to a remote location for printing and tabulation. The 'data' is stored offline in the same way a cold wallet stores virtual coins but by allowing a voter to inspect their vote visually and confirm that the paper is marked as intended provides the trust and security of the good ol' money under the mattress method.

THE 5 BARRIERS TO ONLINE VOTING:

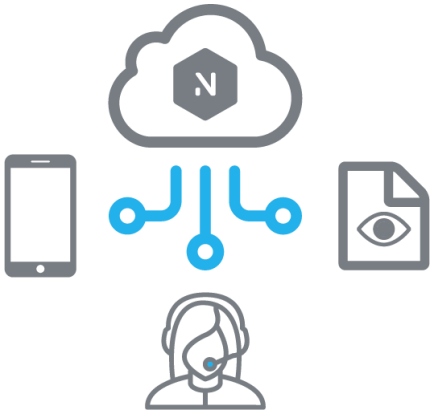
The following are the key concerns critics of online voting systems have identified as barriers both technical and procedural, which must be met to enable confidence in the system.

Certain online systems such as End-to-End Verifiable Internet Voting (E2E-VIV) or Blockchain have been able to satisfy certain barriers separately but not entirely.

Neuvote believes the only solution to these shortcoming rests in its hybrid model of digital and analog security which takes the unique aspects of both methods and utilizes the current advances in communication technology to connect and bridge the gap.

HOW THE HYBRID MODEL WORKS

In traditional voting, the procedure, with all its multiple steps and safeguards *is* the security.



By offering the service to mobile devices, we utilize the increased security over PC interfaces to allow a voter to connect to the system.

The first replication of traditional voting methods is the usage of human scrutinizers who authenticate a voter's eligibility and identity.

By keeping the human element of authentication, we can prevent malicious actors from obtaining and using stolen credentials. Additionally, the method would allow voters to register directly at time of the vote, just as they can do at polling locations currently.

After passing the authentication we can connect the voter directly to their ballot in real time via an End-to-End encrypted channel.

This allows voters to remain anonymous and cast the secret ballot in private.

The voter then can verify that their paper ballot has been marked correctly with their own eyes and can confidently pass the ballot through to tabulation.

This verification does not rely on complicated understanding of encryption algorithms or Blockchain networks. It is a simple replication of dropping your ballot into a box except now accessible from anywhere.

Because our system does not rely on system analysis to facilitate the vote, the only logs remaining are the paper ballot and a receipt of conduct that a voter has passed the eligibility requirement.

This prevents double voting while still allowing full transparency and auditability from elections administrators.

The following sections will examine the specific barriers identified by critics of online voting systems and how this model satisfies those concerns.

BARRIER 1: DATA SECURITY

Data security encompasses the secure transmission, storage and vote tabulation over a network.

The votes, registration database, client side devices, servers, network and encryption protocols used are all possible vectors of attack.

For governments, businesses and financial services these data breaches can be severe, and thusly these organizations spend abundant amounts of resources to prevent breaches and yet still they occur. For an online voting system. A data breach could have a catastrophic outcome.

In online banking, fraud is tolerated, traceable and reversible because whenever data is stored on a computer system it will always and forever be susceptible to undetectable manipulation. Always.

Data security is a high stakes game of cat and mouse between information security analysts and malicious actors. The Stuxnet worm is a perfect example of exceptional intrusion that went undetected for years, using advanced unknown exploits and is highly speculated to be developed by state level actors due to its specific target. An actor with the resources to know of such zero-day exploits has the capability to alter a digital vote and attack a service in a way that cannot be known at time of deployment. With elections being such a high value target to warrant such attacks from state actors with those very capabilities at their disposal, it is clear that standard data security employed by current online voting systems are not capable of mitigating such an attack on democracy.

The incentive of digital state level interference in elections is no longer a hyperbole but a fact. If there ever was a high level election held via online networks it would mean that its data security *must* be able to meet and prevent a state level intrusion attempt.

The vectors of attack for an online voting system are far more diverse than a typical paper ballot, polling booth held election.

Reliance on any one singular defensive strategy whether its E2E encryption, Blockchain or PIN codes mailed to voters is futile in delivering a fully secure online service due to the magnitude of the consequences a breach entails.

The simple truth is that in a democracy, a vote must be regarded as the most sensitive data imaginable and must be treated as such. To store it and rely on its tabulation by digital means only is to disregard the importance a citizens vote has on the fundamental structure of our society.

If storing data digitally is vulnerable for highly sensitive data such as with online voting systems, how can if ever this concern be satisfied?

Solution: Analog Data Security

"Merge your system with something that is analog, physical, or human so

that if the system is subverted digitally it has a second barrier to go through,"

- *Richard Danzig, Vice Chairman RAND Corporation / Former Secretary US Navy*

Intelligence services around the world rely on hybrid models of information transfer and storage due to the highly sensitive nature of the data. Systems implement air-gap network security to move and store data which typically utilize a physical element to protect from intrusion.

If online voting systems and the votes they contain are to be treated with the same regard as our most critical data, a hybrid method must be implemented to ensure that the trust we have in the current system is maintained.

Paper ballots allow for the data to be secured on a physical medium that is verifiable and auditable. A literal paper trail from voter to vote.

The final vote is then stored on a physical medium that is tamperproof by virtue of authenticity alone.

A physical output in an online voting system has the single greatest advantage of not having to store the data on a digital medium and removes the susceptible manipulation element of digital storage. At any point in time, a vote can be physically picked up, inspected and verified that it was cast-as-intended in the same way current auditability occurs.

If storing data digitally produces a high enough target then simply remove that target from the system. The tabulation of votes cannot be hacked if the data doesn't exist digitally or stored on a digital system.

The methodology employed in current online voting systems relies on the ever increasing element of digital data security optimization but by applying a hybrid model with physical output while using those same cryptographic methodologies and E2E encryption verification as the transport protocols, data at rest can be safe guarded from manipulation by creating a true immutable data retention record of a voter's intent.

The fundamental aspect of trust in the system by all invested parties necessitates that trust in the functionality of the administration of an election and the vote that occurs be held as the primary regard. If people don't trust the system it prohibits the ability for online voting to be widely adopted.

The D2P method closes the digital divide by not requiring the average voter to rely on advanced knowledge of various encryption services such as E2E, TLS or Blockchain to cast a vote.

Applying cutting edge information security standards to the server and subsequent

network infrastructure adds a layered approach to the total network security. By removing the high value target from the equation greatly limits an intrusions attacks success.

Keeping the paper ballot allows democratic institutions to maintain the same level of trust as traditional voting but with the increased accessibility of mobile voting.

BARRIER 2: AUTHENTICATION

Authentication in an online voting system entails identifying who a person is, ensuring that the person is who they say they are and validating their eligibility to take part in an election.

Verifying a voter's identity is a challenge for online voting systems because of the lack of face-to-face verification going to a polling booth provides.

Human verification adds a physical, dual factor element to authentication which greatly supersedes any number of numerical voter authentication such as PIN codes or electronic ID's.

It is widely established in information security that username / password authentication is insufficient as a strong security protocol. Some systems suggest physically mailing a personalized PIN code to voters but mail itself is insecure. It can be intercepted, delayed or simply lost and creates a barrier of entry to take part in the voting process.

The concept of government issued electronic ID system also raises concerns due to the fact that these technologies are not fully developed and would have to create, deploy and test the viability of such systems.

With data breaches affecting government records just as often as they do businesses, ensuring total reliance on a catch-all electronic ID system to verify eligibility in the democratic process may not be the best concept.

In addition to the overall voting system online infrastructure, assigning a number to a voter as a valid authentication protocol, whether government or vendor, creates another high value target for exploit or breaches to occur and creates another issue involving stolen ID's being used to cast illegitimate votes.

Proponents of E2E-VIV online voting systems claim that advanced encryption methods are the catch-all solution to the logistical challenges but the possibility remains that an intrusion via sophisticated state level attacks could destroy the integrity of the system as well as the public's trust in digital democratic solutions.

Solution: Visual Verification

Democracies employ the scrutinizer method for casting a ballot at a polling booth because of the human security element.

In traditional voting, having the scrutinizer analyze the ID, info and eligibility of a voter satisfies most security questions. Additionally, seeing the person who will be responsible for counting your ballot satisfies the chain of trust voters must have after they deposit their ballots.

Current technology allows for end to end encrypted video communication that connect people all over the world on a daily basis. If we have the capability to connect people securely in a visual, real time methodology that allows for human verifiable authentication to occur, then this technology lends itself instrumentally to recreate the human security element of a polling booth in a mobile voting system.

By requiring voters to confirm their identity in real time with a scrutinizer via video communication on a mobile device, we can simply transfer the established principles of election administration to the digital age without relying on confusing encryption or insecure PIN code validation.

This human element in conjunction with paper ballot tabulation creates a true analog security obstruction against cyber-attacks by eliminating the two most high value database targets an online system would have, the registration and tabulation.

10 years ago this innovation was not possible as smart phones were still in their infancy but in today's modern society with its widespread adoption of smart phones and their mobile video capabilities, this interface option for human verification is not only possible but easily understood by the majority of people regardless of technological aptitude.

Confirming your authentication in an election system is now just as simple as video calling a friend.

In conjunction with standard voter ID registration systems, scrutinizers can authenticate a person's identity visually as if the person was standing in front of them. This eliminates the reliance on an electronic ID system alone and increases security by maintaining the human element barrier.

This human security element, simulates the same ability to prevent interference in an election as the polling booth method

When systems are digitized, we must maintain the highest level of security. To protect the democratic principles as voting systems move online we must simulate the long standing protocols trusted by time and experience as much as possible.

BARRIER 3: CONFIRMATION

How do you give voters the same level of confidence their vote was submitted as they would experience at the ballot box?

Electronic voting systems in general have a severe deficit in replicating that level of confirmation due to the lack of tactile validation that a vote has been sent securely to an unknown location for tabulation.

With traditional voting the voter has limited authentication that their vote has been tabulated correctly. After the voter deposits their ballot into the ballot box, they entrust the election administrators to ensure that the ballots will be counted and recorded without interference.

This lack of submission confirmation is also evident in online systems where there no human element facilitating the vote and thusly chain of trust developed in the electoral process.

Confirming a vote has been deposited into the count securely is the lowest level of assurance a system should provide to establish trust in the digitized system.

Solution: Visual Confirmation

As this white paper mentioned, utilizing current End-2-End visual communication channels is an innovation not just restricted to authentication via human element but can additionally be used to connect the voter to their paper ballot in real time.

Having a voter not only see their paper ballot marked with their correct intention but also deposited into the count accurately alleviates one of the primary concerns voters have with entrusting their vote in an online voting system.

"To see is to believe" is the mentality we took in developing this innovation because a voter will no longer have to entrust the system works correctly but can simply trust as they watch their marked ballot enter the count by viewing it themselves.

There are multiple confirmation checkpoints to cross before a ballot is permitted to enter the count to reinforce the voter's intent but by facilitating the visual confirmation of a vote it sustains the chain of trust from beginning to the end of the voting process.

BARRIER 4: PRIVACY / SECRECY

Privacy and Secrecy of the ballot are two separate components that enable the anonymity of the vote and voter.

Privacy is the right to cast a vote without oversight and the secret ballot means a vote is anonymous and thusly unable to be associated with a particular voter.

Online voting systems draw an immediate benefit regarding Privacy by allowing a voter to vote anywhere they chose.

In an online voting system, ensuring secrecy is an intricate problem due to the nature of how messaging systems communicate. Data must be told where and how they are to be communicated across the network.

The primary concern with a fully automated network revolves around the issue that to keep track of who, when and how a vote is sent, logs need to be tracked by the system to ensure no double voting occurs and that the messages are getting passed through the system successfully.

Current solutions such as the double envelope method or decryption mixnets where messages are enhanced by advanced obfuscation to ensure that the voter's identity and vote are not linked together are still tracked by the logs necessary for election auditability.

Verification also becomes an issue as the voter has no chain of trust after casting their ballot. To solve this problem, online voting companies provide a confirmation receipt to verify voter intent but this receipt also creates a further security vulnerability and record of activity.

To truly maintain the privacy and secrecy of traditional voting, systems must be designed in a way that minimizes the data that is stored and tracked as closely to traditional voting as possible.

Solution: Designed for Privacy

In the tech industry, big data is worth more than gold unless that company is facilitating voting via a secret ballot.

For an online voting system to be successful in maintaining the privacy and secrecy required, less is always going to be more and the less data stored and tracked, the better.

Just as adding a human element to verification adds a physical barrier to authentication, so does the real-time accessibility of casting-to-tabulation adds an additional mechanism to ensure privacy and maintain secrecy of the vote.

With the D2P mobile voting system, the end point or data storage of the vote is a paper ballot. The identity of the voter is confirmed by a human agent and the voter is then passed to an anonymous ballot marking service which allows the voter to cast their vote and visually see that the paper ballot was casted as intended.

By conducting the vote in real-time including decryption and tabulation, backed with physical paper ballot vote confirmation, an online voting system can simulate the current polling booth and ballot box methodology as closely as possible.

The logs necessary for other online voting systems to maintain auditability are not necessary when the data is being stored on a physical ballot because the paper ballot allows a papertrail to be created between

the action of the vote and the final ballot in the same way as traditional voting allows.

When a voter confirms their ID and passes the eligibility checkpoint, they are presented with a choice to vote. That vote is transmitted in real time across the network in an end-to-end encrypted channel that is obfuscated from the infrastructure facilitating the transmission.

The scrutinizer who authenticated the voter has no access to where the voter was sent over the network and thusly the agent and server mitigating the authentication have no oversight as to the final ballot marking.

By obfuscating the information inside an End-2-End channel, the logs generated by the transmission over the server hold no verifiable information associating a voter's identity to the casted ballot. Even if these encrypted logs were exposed there would be no significant information to extract from them.

By conducting these actions in real time with a visual confirmation by the voter we can safely destruct the logs at time of action and hold nothing more than a receipt of eligibility and the vote.

This solution solves the confirmation barrier facing current methods as the voter can confirm that they have marked their ballot as intended, the ballot has no verifiable elements associating it to the voter and the system administering the election cannot draw any link between the vote and the voter.

BARRIER 5: AUDITABILITY / VERIFIABILITY

For an online system to be fully transparent, it must be capable of allowing election officials to conduct audits against the system to ensure complete fairness in the electoral process.

Online voting allows for benefits that traditional voting cannot provide which can enhance the verifiability a voter would need to feel confident in the system by providing a receipt of record to the voter confirming the voter's intent.

These receipts of record also are a double edged sword as they allow further vulnerabilities to be potentially exposed by linking the vote to the transactional record.

For election administrators conducting an audit, receipts and transmission logs are necessary to ensure the system and election operated correctly.

This post-requisite creates a security paradox in a similar way to backdoor access in encryption algorithms. There is now a key but that key could be used by potential malicious actors.

The logs and receipts required to audit an online system end up creating more records that are vulnerable to malicious actors.

For trust to be established between the voter and election administrators using an online voting system, verifying that their ballot has been deposited and received authentically must be more secure than a simple transaction receipt or confirmation message that their vote took place.

Voters and election observers must be capable of performing in depth audits to confirm that at any point in time the system was not interfered with, no manipulation took place and every vote was counted correctly.

Solution: Paper Trail Auditability

That main deficit with verification and auditability with current online voting systems is that main tenet that any data stored digitally is vulnerable to manipulation.

Despite the intricacies of the transmission process, data is not auditable the same way paper records are. At any point in the process the data could potentially be manipulated to reflect false information. This major flaw in trust is the primary concern preventing online voting systems from being widely adopted in democratic countries.

By utilizing the paper ballot and visual confirmation of transmission, confirmation and vote storage methods outlined in this paper, the final tabulation can be trusted by the voter to be correct and deposited in a format that is identical to the current methods of ballot casting.

To enhance auditability and establish full transparency, the system allows a time stamp of action upon completion of the vote to be kept for administrators or potentially sent to the voter as enhanced verification.

This would allow a full audit to occur by election observers who could draw from sample data sets to test that each individual vote corresponds to a physical ballot.

The only vulnerable data exposed is the time a voter voted. This information only corresponds to the physical paper ballot. Only an official election observer would have access to those two key data points.

These methods combines with enhanced end-to-end encryption and obfuscation techniques would prevent man-in-the-middle observation attempts from viewing the network data transfer.

This auditability innovation is unparalleled in any other online voting system and allows for full transparency and ensures trust in the system by allowing audits to take place at any time including during an election.

CONCLUSION:

This white paper establishes that security in an online voting system is the most prominent barrier facing wide spread adoption.

While the advantages of online voting systems include, cost savings, efficiency and voter engagement, these benefits can never be actualized without maintaining the chain of trust voters have in the security of the system.

By utilizing a system with entrusted security protocols such as analog and multi factor visual verification creates the necessary framework to establish a fully comprehensive and trustworthy digital voting system.

Rather than rely on single software solutions to bring this digital change, the system should amalgamate all available hardware and software advantages to their full potential.

This multi-faceted approach applies the same level of data retention the intelligence community utilizes to transfer and store it's highly classified data. Treating the system with the same regard is not only common sense but entirely practical when the current technological innovations are applied effectively.

Additionally, by treating this technology as an agile development system it can reap the benefit of a dynamic system and rapidly mitigate attack vectors. It also does not have the same deficits that voting machines or locked in algorithms do. Updates, exploits and security holes can be quickly addressed, tested and patched before their vulnerabilities reach the production level environment.

We believe this proprietary Digital-2-Paper method or D2P is the safest way to transfer and store a vote across a network and preserve the level of trust voters have in their democratic electoral institution as it transitions to digital systems.

Whether it is governmental, academic, corporate or union electoral administrators, the Neuvote D2P model is the most secure and simple way to facilitate your vote with the convenience and accessibility that only a mobile device can provide.

For more information on how Neuvote can help you with your election contact us at:

www.neuvote.com

PH – 1-438-863-0234

E-Mail - contact@neuvote.com

© 2019 All Rights Reserved, Neuvote Systems Inc. - Patents Pending