HACKING THE DEMOCRATIC DEFICIT

Why online voting may be the answer to poor voter turnout

The United States has had over two centuries to hone and perfect the democratic process, which continues to be a work in progress. Unfortunately, for the most powerful nation on earth, voter participation is still worryingly low. Despite the highly charged, widely publicized and strongly contested nature of the 2016 Presidential election, only an estimated 57.9% of the eligible US electorate went to the polls, which puts one of the world's oldest democracies in the middle of the league table for voter participation among developed countries.

So why is it that so many Americans are not participating in elections?

Today, technology pervades all aspects of our lives and more than ever, citizens are living their lives online. Whether it is shopping for groceries, banking, filing our taxes or checking in for a flight, we expect to be able to do this with a simple tap and a swipe on our smartphones and tablets, whenever, and from wherever. This in itself has made us less tethered to being in specific physical locations to perform certain tasks and has freed us up to be nomadic and mobile. With this in mind, it is no wonder that when voters are asked to visit a poll station, on a particular day to hand mark a paper ballot, so few turn people turn up.

Change will occur

How could we make voting more accessible and sympathetic to the way in which modern citizens lead their lives?

Harnessing this ever-increasing shift towards digital interaction and allowing people to vote instead from their smartphone, tablet, or laptop, has many obvious benefits. It would undoubtedly help arrest the decline in voter turnout by offering greater convenience, but would also have the added advantage of eliminating some of the most common mistakes that occur with traditional ballots, such as reducing inadvertent voter under/over voting, as well as eliminating counting errors.

It is inevitable, only the timing remains to be determined. Millennials, as they progress in their lives, will simply expect it. Change will occur.

Despite these potential gains, certain computer scientists view online voting as a threat to democracy. They see online voting systems as more susceptible to hacks and security breaches than traditional election processes, and claim that fraud would be harder to detect and control.

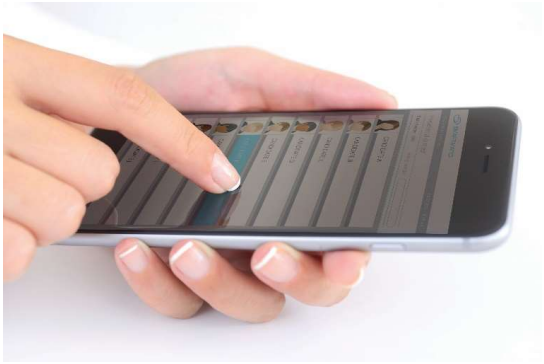
Certainly, not all online voting experiments have gone smoothly. In 2010, the Washington D.C. Board of Elections conducted an experiment in which an online voting system was offered for absentee voters. Prior to Election Day, the District held a mock election and invited interested parties to attempt to compromise its' security. Within 48 hours of the system going live, hackers had managed to take control of the entire system (it should be noted that this was a test and not a real life election and that the hackers were given unrestricted, unencumbered access to the entire system). Experiences like this have caused many people to question whether the security and integrity of online voting can ever be ensured, and governments are understandably cautious of introducing election technology that hackers could potentially compromise.

This is particularly topical given the recent allegations that Russian attackers had hacked the Democratic National Committee email server and had attempted to infiltrate voter registration systems.

Successful online voting

However, despite the failed Washington D.C. experiment, there is a way to engineer online voting systems so that they are more secure than traditional polling methods and potentially arrest the decline in voter participation. Here, the experiences of The Republic of Estonia stand unrivalled.

Since 2005, Estonia has offered online voting in eight Parliamentary, European Parliamentary and Municipal elections with increasing adoption and public trust.



In 2015, Estonian voters cast their ballots from 121 different countries with 33% of the entire electorate casting their ballots online. Estonia's experiences prove that well-built systems can offer convenience to the voter while still upholding the fundamental democratic principles of secrecy and fairness.

So, what is important to consider to ensure secure online voting and why has Estonia been a success?

Online voting has several sub-processes that pose potential challenges:

- **Identity validation**; how can we be sure that an eligible voter is accessing the system?
- S**ecurity**; how can we be sure that the votes are protected from tampering, deletion, addition?
- **Verification**; How can we irrefutably prove that the security mechanisms have worked correctly and the integrity of the votes is demonstrable?

Estonia has invested in building an online voting platform, which has successfully solved these challenges, has been continually enhanced and developed, and features technological and procedural attributes, which are considered as fundamental to ensuring the security and transparency of online elections.

In this whitepaper, we will introduce and explain these as examples of 'best-practice' in the design and engineering of governmental-grade online voting solutions.

Strong voter authentication

A cornerstone to the success of online voting in Estonia is that every voter has a method of strong authentication that eliminates the risk of impersonation and identity theft. Each Estonian citizen possesses an electronic identification (ID) card, which is a credit-card-sized plastic card, which is embedded with a chip and protected by multiple passcodes. This ID card is used by citizens to access a range of government services and to 'digitally sign' a multitude of transactions.

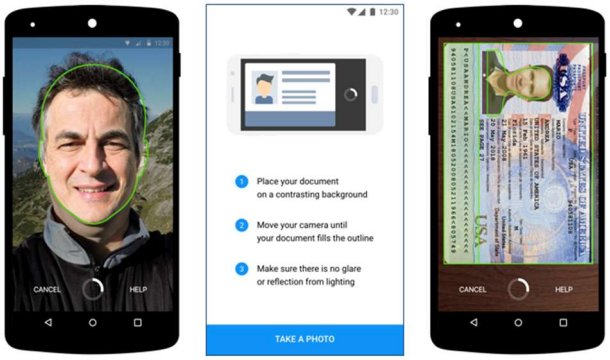
In Estonia, the government retains a profile of each citizen on a central database. When Estonians want to vote, they verify their identity with the online voting system by plugging their electronic IDs into a USB card reader and entering a secret PIN code to verify their identity. The system checks that the biographic and biometric data on their card or device matches all of the information in the voter profile stored by the government. Forging an entire voter profile stored on a unique PIN protected electronic ID is much harder than copying a stolen voter ID number or social security number.

However, given that US jurisdictions do not have electronic ID cards, how can strong authentication methods be applied for online voting in the US?

An option could be the use of identity management solutions, which utilize pioneering mobile facial biometrics. This empowers citizens to create a unique 'digital identity', which can be used to access services such as online voting. These solutions operate as follows:

- The voter registers to vote online by taking a self-portrait ('selfie') using a secure application and the camera on their smartphone.
- The voter photographs some form of agreed, authentic government document (e.g., passport, driver's license etc.).
- Facial biometric software compares the 'selfie' image and the image on the document to compare that they match.
- Biographical information is automatically read from the government document by the smartphone application.
- The images and biographical data are securely cross-referenced with the central database (e.g., DMV) and if a match occurs, a unique, fully-encrypted digital identity is created for the voter and stored on the voters' smartphone.
- The voter is presented with a unique voting credential (PIN).
- For online voting, the voter enters their PIN and takes another 'selfie', which is compared with the digital identity stored on their smartphone and if they match, the voter is identified and their relevant ballot presented on their smartphone.

This method of registration and authentication provides an incredibly robust method of eliminating voter fraud, impersonation and identity theft and provides a simple and intuitive experience for the voter to securely cast their ballot.



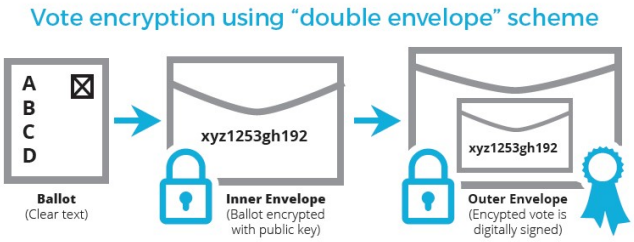
The importance of end-to-end ballot encryption and the digital 'double-envelope'

A critical process in online voting is securing and transmitting the vote to the digital ballot box. This is the step that many experts opposed to online voting argue that hackers would be able to exploit. However, with the use of application level cryptography, which is not commonly used in most web applications (including online banking), it can be made highly secure to eliminate vote eavesdropping and tampering.

The best way to safeguard digital ballots is by using public-key encryption. This technique uses two cryptographic keys—a public key known to the sender (in this case, the voter) and a secret private key known only to the recipient (the electoral board).

Once the voter has made their selection, their choices are encrypted on their computer (before they are transmitted) using the election public key. Once the ballot is encrypted, it is then 'digitally signed' using their unique digital identity to create a digital 'double-envelope'. The inner (ballot secrecy) envelope maintains the privacy of the vote and the outer envelope assures that the vote

was submitted by the eligible voter, and in this respect the process mimics that of postal voting, albeit with far stronger protection. Rather than paper, the inner envelopes use a strong encryption algorithm to convert the plain text of a candidate selection (for example, “John Doe”) into a randomized string of digits and letters called ‘cipher-text’ (for example, 36dhfi8wfhzm6fh2alg8tbsd82jfn8q7374hw7d2hgb528) that only the private key can interpret. The outer envelope relies on a similar technique to scramble the voter’s identity to produce a secure digital signature.



Once signed and encrypted, the voter sends his/her vote to a digital ballot box through a secure connection that relies on a popular Internet protocol known as Transport Layer Security (TLS). With this protocol, the connection between the voter’s computer and the digital ballot box is established using another form of encryption called ‘symmetric cryptography’. The voter’s browser and ballot box agree on a cipher suite, or a combination of authentication and encryption code, as well as key exchange algorithms that they will both use to securely send messages, prove their identity to one another, and trade random numbers to create a master secret. The browser and ballot box then use this secret to generate session keys, which are used to encrypt and share data. This is all done at the start of a session before the vote is transferred.

Using this method, the vote preferences are fully protected from tampering and voter privacy is maintained and this approach is considered a ‘baseline’ requirement for governmental online voting.

Mixing and distributed key protection

All cast voters, which are received by the digital ballot box, remain encrypted until the election has finished. Following closure of the election, the encrypted votes are transferred to a ‘clean’ air-gapped server where they are prepared for counting. The system strips the voter’s digital signature from the ballots (outer envelopes) to reveal the encrypted votes (inner envelopes). The votes are then cryptographically ‘shuffled’ to randomize the order in which they were cast and which makes it impossible for an eavesdropper to correlate a vote with its corresponding digital signature. The shuffling is normally achieved by passing the encrypted votes through a mixing network, or “mixnet.”

In a mixnet, message routing protocols send messages through a chain of proxy servers or nodes, with each node accepting messages (in this case, votes) from multiple servers, re-encrypting them, and sending them in a randomized order to the next node in the chain. Using this process, voter anonymity is fully protected and mathematical proofs are created which verify the integrity of the votes through this process.

The votes can only be decrypted using the election private key, which would clearly be of great interest to anyone seeking to hack or subvert the election.
However, the encrypted votes are protected by the fact that the private key does not actually exist at this stage.

The private key can only be generated by bringing together members of the electoral board who each have a share of the private key, and recombining them to create the full key.

In this situation, the private key is divided into pieces that are distributed on a set of PIN-protected physical tokens, such as smartcards or secure USB devices. The tokens containing the pieces of the key are then distributed to a number of members of the electoral board. Without the reassembled key, it is impossible to decrypt and count the votes. After the polls close and the votes are mixed, these members meet at the election office and insert their smartcards or USB devices into the decryption server. They enter a PIN to unlock their device, and their share of the election private key is read and combined with the other shares to recreate the private key. Only then can the clear text voter preferences be ascertained and counted.

Finally, the votes cast in an online election must be automatically tallied by a separate vote tallying system, which is tested for logic and accuracy before the election and validated for correctness by independent auditors.

"Doveryai no Proveryai" - Trust, but Verify

Having an online voting system, which is fully-secure through the means of end-to-end encryption is critical to ensuring the integrity of the election but providing tools to irrefutably prove that the security measures are operating correctly must also be present.

'Trust, but verify' is the translation of a Russian proverb ("Doneryi no proveryai"), which became well known when used by former US President, Ronald Reagan in the context of nuclear disarmament at the cessation of the cold war. In the context of online voting, while end-to-end encryption can provide robust protection for the privacy and integrity of online ballots, it is important to provide voters with a mechanism to verify that their vote was received in the state that it was cast to prove that the security procedures have operated correctly to protect the vote from manipulation. This is where 'voter verification' comes in.

This can be best achieved through the use of verifiability protocols which permit the voter to check the validity of their cast vote on a separate digital device to the one they voted on. In the case of Estonia, voters can verify their vote through their smartphone as follows:

- When a voter casts their ballot from their computer, the digital ballot box receiving the vote generates a unique voting receipt, which is displayed as a QR code on the voter's computer. Using their smartphone, and a certified verification application, the voter scans the QR code, and performs a cryptographic operation, which displays the contents of the vote that was logged by the ballot box. The voter can easily see that her vote was successfully and accurately cast.

By using a separate physical device to verify a vote cast on a laptop, or vice versa, the voter can also identify and mitigate potential "man-in-the-middle" attacks in the unlikely event that the voter's computer is compromised by a hacker. Any potential attacker would need to institute a coordinated attack on both the voting device and the verification device, which would be virtually impossible in practice. This is an improvement over traditional mail-in ballots, which give voters no way of verifying whether their ballot has reached its intended destination unless they pay for certified delivery.

Introducing Blockchain

Blockchain technologies have been receiving a wealth of publicity from the technology community as a mechanism to protect digital transactions. While the majority of the development and application of Blockchain has focused on verifying the integrity of financial transactions, the tamper-proof properties of Blockchain offer an opportunity to use it to prove the integrity of a multitude of digital transactions, including online votes.

A Blockchain is an open ledger or database that relies on a community of users to record timestamped transactions in a continuously growing record of 'blocks', and post them to a public bulletin board that is available to anyone online. The legitimacy of each new transaction is evaluated by every user based on an agreed protocol. A transaction is only added to a new block of the chain once it has been verified by a majority of users. And rather than being kept in one place, a copy of the entire Blockchain is stored on every user's server so that no single user can alter a past event without other users finding out.

In the context of online voting this public bulletin board records a cryptographic "hash" of each vote, which has been sent to the digital ballot box. The hash is created by taking the encrypted and digitally-signed vote and passing it through a cryptographic hash function to create a string of bits of a fixed length, called a digest. By finding his/ her digest listed on the bulletin board, a voter could verify the presence of their vote in the chain without anyone else knowing which vote she cast. At the same time, it is impossible for anyone to add, remove, or modify votes without corrupting the Blockchain. And after the polls close, another Blockchain is created from the votes passed through the vote-counting application, and compared with the public bulletin board's Blockchain, to prove that the online voting system had operated correctly.

Summary

There is a reason to feel optimistic about the future of online voting. Estonia continues to develop its' online voting platform to take advantage of advancements on cryptography and verifiable protocols, Switzerland and Australia continue to develop their own experiences and in the US in 2016 the Utah Republic Party offered online voting for its presidential preference contest.

With advances in sophisticated encryption methods, such as post-quantum cryptography, verifiable cryptography and mobile digital identity management, the remaining challenges of secure online voting are being solved more effectively than ever. Despite concerns from some computer scientists, electoral management bodies and democratic governments throughout the world consider online voting to be not a case of if, but when. The challenges of identity validation, security and verifiability are being solved in 2017.

Maybe in 2020, we'll see the first U.S. president elected by iPhone.

About the Author

Mike Summers is the Program Director for Internet Voting at Smartmatic, and Director of the Smartmatic – Cybernetica Centre of Excellence for Internet Voting.

Founded in the U.S. in 2000, Smartmatic is a leading provider of voting technologies and solutions. The company has managed elections across five continents, processing over 3.7 billion votes. Smartmatic is headquartered in London, UK, and has offices in Boca Raton, Florida.
www.smartmatic.com