Electronic Voting Keeping in View the Democratic Principles

Mr. Junaid Akram[*]

Abstract

Voting has traditionally been performed by casting paper ballots in public polling places. However, advancements in computer technology in the latest decades have enabled voters to cast their votes electronically. By 2016, eleven different countries have made various trials enabling voters to cast votes on the internet using personal devices. Internet voting has become a considerable topic of discussion in the scientific community, with regard to both technology and democracy. Any election is required to preserve a certain set of democratic principles. Consequently, allowing internet voting is prone to numerous challenges which must be addressed. This paper explores that nations where trust in the government is limited, election experts should consider whether internet voting with end-to-end verifiability can preserve the integrity of election results and increase public confidence. Additionally, nations making trials with internet voting should investigate the possibilities of using recent technological advancements like blockchain in internet voting systems.

Keywords

Voting, Democracy, Public Polling, Computer Technology,

Introduction

Elections have been the most important feature of democracy since the introduction of Athenian democracy in the 6th century BC. Although the act of voting was then unusual and only considered benefiting the wealthy and people of power, it is now crucial for any government elected by the people. However, elections can only be democratic if

[*] M.Phil. scholar, National University of Science and Technology, Islamabad

citizens are provided with the ability to vote. Therefore, suffrage, or the right to vote, is vital to any election. Despite this, universal suffrage is not taken for granted in every society.

As society advances by innovations in technology, progress is made in the field of voting. Historically, voting was performed in public and later with mechanical machines using punch cards. Most elections now enable voters to cast votes using paper ballots in public polling stations. Additionally, remote voting by postal mail allows citizens living abroad and voters who cannot access a polling station to cast their votes.

Advancements in computer technology in the latest decades have enabled several nations to offer electronic voting. More recently, with the increased use of the internet in society, both private and public services are provided through increasingly efficient, online solutions. The internet enables citizens to handle their finances, apply for admission to schools, social benefits and other important services. Consequently, they may now expect to cast their votes using the internet.

In the past few years, internet voting has enabled voters in numerous nations to cast their votes from their computers with instant verification. Internet elections have been conducted on a national scale in Estonia bi-annually since 2005. Switzerland has been conducting trials with internet voting for citizens living abroad since 2008. Norway has conducted trials with internet voting in both 2011 and 2013. Other European countries, e.g. Sweden and the UK have proclaimed their interest in conducting internet elections. This growing interest suggests that multiple countries are possibly going to conduct trials with internet voting in the near future.

The ability to cast votes remotely is one of the key features of internet voting. According to the US Vote Foundation study, remote voting is both a necessity and a yearning for voters (Murray et. al., 2015). It enables citizens living abroad, military personnel and people with physical disabilities to vote without visiting a polling place. In addition, it may increase voter turnout and decrease administrative overhead. The use of the internet for remote voting provides instant receipt and verification of votes.

Limited accessibility is a significant challenge for several voters and is one of the most pronounced reasons for conducting elections using the internet. Although adjustments are made to provide every eligible voter with the opportunity of voting, they are not always sufficient. The National Institute on Intellectual Disability and Community in Norway states there are still several factors limiting the accessibility for people with disabilities (Wollscheid & Hammerstrøm, 2012). In an article published on their website just before the municipal election of 2015, they identify several limitations like the organization of physical meet up and the forfeit of privacy if voters require assistance to vote. In addition, they remark that personnel may hinder unbiased vote participation by withholding information, because they may believe people with certain disabilities do not understand the impact of participating in an election. Although difficult to prove, it is still an important observance for the argument of internet voting, which could possibly prevent such prejudice.

Absentee voting lacks the possibility of voting securely and with confidence. Postal voting is used in several elections around the world and is a relatively low risk method of voting. However, it provides no verification or receipt of whether votes are received or not. Because they are sent by postal mail, often overseas, they would also need to be received by the respective government before tallying on Election Day. Delays which would not be present in an internet voting system may cause the vote to arrive too late and be discarded. These facts are arguments for the implementation of a more universal voting solution, which can provide the same confidence of vote reception as a vote placed in a polling place. It can be argued that the most feasible and obvious replacement is to introduce internet voting for absentee voters.

Until Estonia became the first country to offer internet voting nationally in local elections in 2005 (Broache, 2016), electronic elections had traditionally been conducted through the use of voting machines in polling places. A study made by Voting Systems Technology Assessment Advisory Board (VSTAAB) in California in 2006 called Security Analysis of the Diebold AccuBasic Interpreter (Wagner et al., 2006) proved the direct-recording electronic (DRE) voting machine used in several US elections until 2004 to be easily modifiable. This and several other systems are part of the reason that electronic elections have been and still are met with scepticism by scientific communities. Despite criticism, the development of electronic voting solutions has not ended. On the contrary, it has bloomed and in recent years, technological advancements in the field of cryptography has proven to be advantageous in the development of new systems and protocols for providing more secure and transparent electronic elections.

Elections are founded upon a set of democratic principles. Among the most important are providing sufficient voter privacy to prevent undue burdening and ensuring all registered votes are included in the final tally. Another important principle is transparency, enabling citizens to verify that elections are conducted without any irregularities. Preserving democratic principles is the primary goal of an election and is achieved through multiple features. In an internet election, such a feature can be cryptographic mechanisms which enable electronic votes to be protected from unauthorised disclosure both in storage and in transit.

Trust is another important property of a democracy. In a traditional paper election, voters place trust in government officials and the lawful conduction of election procedures. Despite this, the same trust cannot be applied to an internet election. In fact, recent developments in the field of electronic elections demand trust to be replaced by undeniable, mathematical verification. Voters must be provided with the ability to verify that their votes are included in the final tally, referred to in the literature as end-to-end verifiability. The internet voting system Helios has implemented this feature to its fullest extent. The Norwegian internet voting trials of 2011 and 2013 implemented properties of it with the goal of transparent and secure internet elections.

Threat Assessment of Electronic Voting

The goal of a threat assessment is to identify when and where vulnerabilities are present in a system. It also attempts to identify how vulnerabilities can be exploited and by whom (De Faveri et al., 2016). A threat assessment purposefully does not include any countermeasures, because the purpose is to identify the environment of the system in its most elementary state.

An internet voting system consists of three connected environments, including the voter’s computer, the internet and the voting system. Votes are cast using the voter’s computer and transferred across the internet to the voting system where they are stored and tallied. All three environments and the information they process are susceptible to various risks. The term risk is often associated with information security incidents, which can be deliberate actions, negligence, accidents and disasters. Elections are by their very nature prone to deliberate actions with malicious intent, referred to as attacks. The entities performing them are referred to as threat actors. Because internet voting is performed on an open channel, both the amount of possible threat actors and attack vectors significantly surpasses those of paper voting. In an election, threat actors can be both internal and external. Internal actors are located on the inside of the system which they act against. In the voter’s computer that is the voter or any legitimate entity with access to it. External actors of the voter’s computer are anyone from an outside network with access to the voter’s computer through, e.g. malicious software (malware).

The internal actors of the voting system are the system operators, which have authorized access to the infrastructure and components of the system. External actors of the voting system are entities without authorized access, with the exception of the public voting client.

A challenge of allowing votes to be casted using the internet as opposed to paper is the difference in attack surface. In a paper election, surveillance and control of the ballots prevents any large-scale manipulation. When votes are electronic, a potential attack scales significantly higher. Consequently, a threat actor with access to the system can potentially manipulate vast amounts of votes simultaneously and in a worst-case scenario such an attack is so complex it subverts detection. In a paper election, external attacks are less feasible and an internal attack would require a conspiracy of some proportion, consequently increasing the likelihood of detection.

Voter’s Computer

In a traditional paper election, the voter is in a polling place monitored and controlled by functionaries. The ministry report electronic voting - challenges and opportunities explains that because this sufficiently enables voting without undue burdening or vote manipulation, it is considered a controlled environment (Department for Communities & Local Government, 2006). Further they explain that voting outside a polling place is considered an uncontrolled environment. When votes are casted in such an environment, e.g. a voter’s computer, voters are no longer sufficiently protected from undue burdening and votes are significantly more susceptible to manipulation.

Possible internal attacks in the environment of the voter’s computer are voter coercion and the buying and selling of votes. Allowing voting from an uncontrolled environment enables situations where applying pressure to a voter is significantly easier than when voting in a polling place. The possibility of passive attacks also increases when voting from personal devices, because family members, friends or otherwise curious persons may be able to observe votes being casted, consequently breaching voter privacy.

A possible external attack on the environment of the voter’s computer is theft or forgery of voter identity. This can occur electronically, but also physically by stealing poll cards sent by postal mail. Gaining access to voters’ authentication credentials would enable an attacker to cast votes using the identities of legitimate voters. Such an attack is however demanding for the attacker, does not scale well and is easily detected.

A far more probable scenario is an attack on the software of the voter’s computer. Operating systems are very susceptible to malicious software, and a compromised computer would allow an attacker to both spy on the voter and take control of the computer (Jefferson et al., 2004). If an attacker is able to spy on the voter during voting, privacy is forfeited. More importantly, an attacker controlling the computer can prevent a vote from being sent, or manipulate the choice of the voter before it is submitted. Microsoft’s Security Intelligence Report from July to December 2013, made a six-month observation regarding malicious software on Microsoft Products (McGuire & Dowling, 2013). This measurement revealed that 21.2% of all computers running Microsoft products with detection tools had encountered malicious software in that period. Considering Microsoft still has the majority of the operating system market share, this evidence supports the assumption that large amounts of voters' computers could be infected with malicious software.

The issue of compromised computers is a significant difficulty for internet elections, because it is so hard to prevent. Considering voters' computers are in an uncontrolled environment, there is a limit to what election officials can do to remedy this issue other than providing voters with training and knowledge regarding computer security. Nevertheless, it is fair to assume that an attacker with enough competence to take control of a voter's computer is able to make such actions undetectable to the voter. Consequently, such attacks can result in voters confident in having cast their votes, but oblivious to the manipulation which has been performed.

The Internet

The internet is a public channel and voting communication traverses numerous intermediary servers, routers and links before being received at the voting servers. Consequently, it is reasonable to assume the vote is intercepted and possibly modified while in transit. A compromised vote both harms voter privacy and the integrity of the election (Marias et al., 2012).

Although protocols like Transmission Control Protocol (TCP) attempts to prevent network traffic on the internet to be corrupted in transit, errors may still occur preventing the vote from being delivered correctly (Bellovin, 1989). Despite such issues being difficult to mitigate for internet voting systems, they should employ techniques to discover if votes are lost or corrupted while in transit from the voters' computers to the voting system.

One of the most severe attacks on an internet voting system is redirecting voters to false websites. Such sites present themselves as legitimate by having indistinguishable design and Uniform Resource Locators (URLs) similar to the real voting website (Wardman, 2011). An attacker can use such sites to harvest voter credentials or to discover voters' political intentions. If the attacker acquires voters' authentication credentials, they can use them to authenticate to the real voting system and cast votes on behalf of legitimate voters. Votes cast on a false site would naturally not count either, so voters may believe they have voted when actually they have not.

Attacks using false websites are easy to perform and scale remarkably well (Harwood, 2010). Creating and deploying a website with legitimate certificates is simple and spreading its URL through social media channels and e-mail allows the attacker to quickly advertise it. Although such an attack will presumably be detected quickly, huge amounts of voter data can be harvested if the attack is timed correctly, e.g. on election day. All these factors contribute to make false voting websites one of the most severe attacks on an internet election.

Voting System

The voting system is where votes are collected, stored and tallied. It is prone to multiple internal and external attacks. Internal attacks can be performed by system developers, system operators or other insiders like observers or auditors (Al-helali & Hameed, 2010). Numerous different organizations and individuals may have interest in disrupting or manipulating an election and may therefore attempt both internal and external attacks.

System developers may deliberately implement features to manipulate votes, redirect them or prevent them from being counted. However, due to the complexity and size of a voting system implementation, its development is also prone to errors and negligence. Auditing large amounts of source code is demanding and the challenges of this process may enable errors and bugs to remain undetected (Hao & Ryan, 2016).

System operators are perhaps the most vulnerable part of a voting system. They are competent personnel with authorized access to vital information and infrastructure (Rakodi, 2003). Although they may have personal gain from compromising an election, their role makes them targets of external attackers who want to gain access to the system, either by fraud, coercion or the promise of compensation. An attacker with sufficient access to the system can potentially compromise the secrecy and integrity of votes as well as system availability.

Both the confidentiality and integrity of votes are vulnerable during tallying. Confidentiality may be compromised in the tallying because it involves removing the personal identification from votes before counting them (Gritzalis, 2002). System operators or observers may gain access to information allowing them to discover the intentions of voters. The integrity of votes may be compromised if a machine tallies wrong by design or is sabotaged. Not being able to count results accurately and quickly is considered a compromise of the availability of the system and can create electoral distrust.

Hostile individuals may wish to disrupt the system for personal reasons or steal data for publicity (Denning, 2001). Hacker groups may also seek to attack the system to protest against the election for political reasons or to display discontent with internet voting. Criminal organizations may exploit the system to gain personal data. Foreign intelligence services may seek to disrupt the election or manipulate it for political reasons. Terrorist organizations may wish to compromise the election to gain electoral information or manipulate its outcome.

There are multiple methods available for attacking the voting system. A somewhat undefined "hacking" may be performed, which involves a threat actor gaining unauthorized access to the system (Tkacheva, 2013). The possibilities of such attacks are vast once access has been gained, e.g. a complete compromise of election results or destruction of important information like votes. A possible attack on availability is a distributed denial of service attack (DDOS), which involves disrupting the election by making the voting client or other underlying systems unavailable, thus preventing legitimate voters from casting their votes. With regards to accidents, both equipment and infrastructure may fail, potentially leading to service unavailability and loss of information (Starr et al., 2010). Additionally, natural disasters may cause equipment or infrastructure failure.

Trust in Electronic Voting

Trust is defined as "a positive expectation regarding the behaviour of somebody or something in a situation that entails risk to the trusting party" (Marsh & Dibben, 2003). The possible levels of trust are trust, mistrust and distrust where they all vary over time. An individual with trust in an entity is cooperating with it. An individual with distrust is not cooperating with an entity, and may even try to act against it. Mistrust is usually a transition state between trust and distrust.

In a democracy, governmental power is granted by public election (Habermas, 1994). To accept the government allowing internet elections, voters need complete assurance of fair conduction and correct election results. Any doubts about the integrity of the results of election procedure may lead to distrust in the election, government and democracy. In the context of internet voting, trust has two dimensions.

The first dimension is the trust the public places in the election being conducted without forfeiting democratic principles. In a paper election (Sztompka, 1999) this trust is usually earned if the election has proven itself to be transparent and reliable, by previously conducting elections without any proven manipulation or corruption. This dimension of trust does not rely on the voting method of the election being neither paper nor electronic. An important measure to build this kind of trust is transparency. In an internet election, the electorate must be able to trust the electoral process enough to accept results without any doubts of its legitimacy. Internet voting is not feasible if the electorate does not trust the electoral process to be correct (Cranor & Cytron, 1997). Providing transparency about the project management and the implementation of the voting system contributes to building trust in the election.

Lack of transparency in the election and its services can contribute to decrease trust. If documentation about the system, its equipment and services are not publicly available, voters are required to trust the promises of vendors, the government or other controlling instances (Moynihan, 2004). This requirement is not a satisfying assumption of trust. Necessary information about the election and its services should be public so it can be inspected by election experts, observers, voters and other third parties. The other dimension of trust is the trust which voting authorities and electorates place in the assumption that the voting system is operating according to specification. Any internet voting system must be accurate in the sense that the election results reflect the intentions of voters without any discrepancies. Internet voting systems use computers and software operated by humans, which are all prone to both errors and deliberate manipulation (Kohno et al., 2004). Their assumption of trust needs to be rooted in something less prone to such occurrences. Because trust cannot be completely eliminated, the goal therefore becomes to design a system which minimizes the requirement of trust to a limited set of players and components (Ramchurn et al., 2004).

When voting in polling places using paper, voters receive immediate verification of vote recording. Their ability to personally deposit their votes in the ballot box builds confidence in that their votes are cast correctly (Oostveen & Van den Besselaar, 2004). From that point in time, voters trust that their votes are counted in the final tally, under the presumption that the ballot box will be under surveillance until tallying. Voters trust this system because it is transparent and easy to understand. When voting electronically, voters lose the tangibility and transparency normally provided by paper voting (McGaley & McCarthy, 2004).

Because any computer system is very much like a black box, gaining trust is difficult. In computer science, a black box is a system where the user can see the input and output, but has no insight to its inner workings (Diakopoulos, 2015). In 1984, computer scientist Ken Thompson wrote a short technical report where he demonstrated a computer programmable to manipulate data and hide all traces of manipulation (Jensen, 2014). Similarly, when voters cast their votes using a computer connected to the internet, they have no actual knowledge of the proceedings of vote inside the computer, while in transit over the internet or when it is stored at the voting servers. This makes it difficult for voters to trust such a system, because they have no guarantees it works as intended unless provided an undeniable proof.

Democratic Principles

Internet voting systems are subject to fulfil the same functions and requirements as paper and mechanical voting systems. Therefore, they must also meet the same standards for retaining democratic principles. Because no international standard exists for performing elections democratically, governments often define their own principles and requirements. However, a certain baseline of democratic principles is stipulated by OSCE.

In their handbook for observation of new voting technologies (NVT), OSCE defines seven key principles in the use of different technologies for the conduction of elections (Organization for Security and Co-operation in Europe, 2013). The seven democratic principles are defined for the observation and use of elections featuring NVT, but apply to any election regardless of technology. The principles are sufficiently justified with reference to OSCE’s own 1990 CSCE/OSCE Copenhagen Document (Wright, 1996), which outlines human rights and fundamental freedoms. The stipulated principles are therefore well reasoned for and a credible source for the description of democratic elections. Another source providing credibility to these principles is the Council of Europe. In their 2011 document Guidelines on transparency of e-enabled elections they confirm that their principles of electronic election coincide with the OSCE principles, especially regarding transparency (Wenda & Krimmer, 2016). This further strengthens the notion that the principles described in this section are based on information from credible sources.

Secrecy of the Vote

Secrecy of vote as a principle involves the assurance that no voter can possibly be associated with a vote. Neither should voters be able to prove how they voted. If a voting system provides receipts or any other kind of confirmation to a voter that a vote was cast, these features should be designed to ensure that the secrecy of the vote is still retained.

Secrecy of a vote is one of the most crucial democratic principles, because an election which does not fulfil this criterion cannot be considered democratic. Conducting a democratic election is impossible if the choices of voters are disclosed, as it eliminates freedom of choice and creates the possibility of coercion, intimidation and persecution based on political preference. Consequently, any democratic election must fulfil this requirement.

Integrity of Results

According to both the OSCE handbook and the OSCE Copenhagen Document, integrity of results is a principle which must be preserved under any circumstances. It implies a chain of actions are performed to ensure an honest counting and reporting of votes by the end of the election. Not only must all votes be appropriately counted and reported, but no vote shall be unjustly added or subtracted from the results neither before, during nor after tallying. There should not be any errors in the process, but if any are present, they should be detected and managed according to strict procedures. In most electronic election systems this involves both electronic detection mechanisms and observation of the entire process by unbiased third parties.

When providing election results, the electorate must be provided with undeniable verification of the correctness of the tallying process. Such verification can be provided by protocols of verifiability or manual recount. If a system is reliant on the trust of election officials, vendors or other personnel involved in the election, it does not provide sufficient integrity. Additionally, any verification mechanism should not be able to compromise the secrecy of the vote.

Equality of the Vote

Democratic elections build upon a presumption of political equality. The principle of equality of the vote requires that every voter's opinion is equally valuable and that no voter is able to cast more than one vote. Every vote should have the approximately same value and not differ within the same district the votes are cast in.

Equal ability also presumes no eligible voter is prevented from participating in the election. Not only does this involve that no voter can cast more votes than other voters, but also that legitimately cast votes cannot be removed from the system. Consequently, the principle overlaps with the principle of integrity of results. Although some systems allow for casting votes multiple times to prevent coercion and vote purchasing, such systems must be able to handle these features accordingly. The system must also be able to prove that the principle of equality is not violated in any way.

The principle also addresses the fact that voting should be available to all eligible voters. Any electronic system used in the voting process should not discriminate or prevent certain groups from participating in the election. If multiple combinations of voting methods are used in an election, like the possibility of both electronic and paper voting, both systems should be equally available and accessible. Any difference in the accessibility of voting methods can endanger the principle of equality.

Universality of the Vote

The principle of universality of the vote presumes all eligible adult citizens are provided with the opportunity to vote without difficulty. This especially applies to voters with disabilities and absentee voters. When an electronic system is used for voting, paper voting should be provided in combination with it, because electronic devices may be difficult to use for some voters. This principle is therefore closely related to the principle of equality.

Transparency

Transparency is one of the most demanding of all the democratic principles of an election. It is the key to verifying that elections are conducted according to law and according to the other democratic principles. This contributes to the election becoming predictable and understandable for the electorate, consequently increasing trust in the election and the democracy.

Transparency as a principle is realized by making an election observable. Observability is achieved by allowing any third party to observe and inspect any part of the election. It is important that the observance is made possible and simple, by providing ease of access to the observers and making sure documentation is available and understandable. Observers should never interfere with the election processes, but still have the ability to inspect and verify the election.

Accountability

Accountability means that any person involved in the election process is subject to be held accountable for their actions. This includes not only election officials and security personnel, but also software developers, auditors, vendors and any other entities involved in the election. The election officials, often a government agency should have responsibility for the totality of the election, including control over any employed third parties and systems. Accountability also involves having a detailed recollection of how, when and where election operators and other personnel interact with the voting systems.

Public Confidence

Public confidence is another significant principle of public elections. In order for election results to be legitimate, any participant of the election must be able to understand how the voting system works. Additionally, the process must be auditable by any third party. Consequently, this principle is retained only if the other principles are sufficiently preserved by the election. Public confidence can be difficult and time consuming to build, but without it democracy would be impossible to practically enforce. A measure significantly improving public confidence is including the electorate in the election process by providing sufficient transparency and proving the correctness of election results with undeniable verifiability.

Comparative Analysis of Electronic Voting Systems

Country	E-Voting	Company	Election Type	Electoral System	Introduced Year	Year Used	Software Used	Hardware Used	Problems
India	668 million	BHEL	State	FPP	2001	2009/2004/2003/2001	EPROM	EVM	None
Belgium	3.2 million	Steria	General & Municipal	Open PR-List	1994	1999	Digivote, Jites, Stesud	DEVS	2003: 500 Power and Computer failure
Brazil	66 million	UniSys & Diebold	All Govt. Level		1996	1996/1998/2000/2002	GEMS	GX-1 integrated processo	None
Australia	0.218 million	Software Improve	ACT federal	PR-STV	2001	2001	eVACS	PCs	None
UK	1.5 million	SVS	Local Govt	FPP	2000	2000/2003	AVC	DRE	Mobile e voting
Spain	3000	Indra	Municipal	PR-List	2002	2003	SIRE	SIRE System	None
Canada	98000	CanVote	Municipal	FPP	2002	2003	CanVote-on Linux	CanVote Internet	None

The Future of Internet Voting on a Large Scale with Stability

Internet voting also has multiple challenges yet to be addressed. The development of voting technologies, election procedures and cryptographic techniques may contribute to improving internet voting.

Smartphone as Voting Device

The latest decade has been distinguished by the widespread availability of smart- phones. According to a report1, 72% of phone owners own a smartphone. Voters may expect that with such a wide use of internet enabled devices with access to all kinds of services, like banking, entertainment and governmental services, they would be able to use these devices to cast votes in an internet voting solution. As a usability study conducted by the US Vote Foundation points out, voters are used to rich online experiences from both website services and smartphone apps and may therefore expect an equally modern voting experience. Additionally, because most smartphone operating systems have accessibility tools installed by default, they accommodate users with disabilities. Therefore, enabling voting through an even more available mechanism than computers may both increase availability, accessibility and fulfil the expectations of voters.

Introducing smartphones would however create issues of delivering return codes securely. The current solution uses the SMS channel because it is a personal device outside the voting environment. With a smartphone, the SMS is potentially delivered to the same device as the voting, thus no longer providing two factor security. Therefore, if proposing the use of smartphones for voting, another means of return code delivery must be suggested. Additionally, casting votes using computers is still an available voting method. Consequently, the separation between these voting methods would have to be clearly identified, so the delivery of return codes and casting is never performed on the same device.

In Norwegian Electronic Elections 2013, the Ministry wanted to prevent voters from using their smartphones to cast votes on the same

[1] pas.org.pk

device they received SMS return codes (Meter, 2017). Bull (n.d.) explains that consequently, they banned voting with smartphones by comparing the user agent of the web browser against a blacklist. Although not a very durable solution, it kept the majority of voters from using smartphones to cast their votes. At the time, the feature of requesting desktop sites on mobile operating systems, which spoofs the user agent, was not yet introduced for Safari on iOS nor commonly known in various Android web browsers. Because this feature is now available as built in functionality of most smartphone operating system's web browsers, internet voting should adapt, rather than trying to prevent this any further.

The SMS channel also has constricted with regards to message length and provides no guarantees of delivery. Additionally, message delivery is prone to potentially significant delays and the possibility of falsifying sender is relatively easy (Feroze & Basharat, 2011). Some mobile network operators provide services through web interfaces to send and receive SMS, which allows for the disconnection of voting device and return code delivery device. This does then however in fact rely on voters actually having access to a smartphone and another device for verification, thus limiting the intended universality of introducing smartphones in the first place.

Mobile devices and their operating systems contain extreme amounts of personal information, like email, banking details and other important credentials. For this reason, they are developed with security in mind (Anderson, 2008). Current devices provide secure execution environments and security enclaves, making manipulation both logically and physically harder than the average home computer. A Trusted Execution Environment (TEE) is a secure separated part of a smartphone processor, allowing the execution of code in an environment separated from the mobile operating system. The paper "Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give Me?" identifies multiple security properties and use cases for TEE (Vasudevan et al., 2012). Such an environment provides security features, namely isolated execution, secure storage, remote attestation, secure provisioning and trusted path. All these features are part of providing integrity and confidentiality of information, which can potentially be credentials and internet votes. Because of its strong security features, it allows users to place a larger degree of trust in it than in a computer and could potentially be used for smartphone voting.

If enabling smartphones for voting is developing and deploying an app., this app would be assuming the properties of verifiability and also be able to both authenticate voters, allowing them to cast votes and potentially provide cast-as-intended and stored-as-cast proof on one single device (Heiberg & Willemson, 2014). This would have to still preserve secrecy and integrity of votes by enabling voting to be performed without manipulation, preferably by using mechanisms of vote verification. Justifying the use of only a single channel for all these features would however require significant guarantees of the integrity of the system, through the use of mechanisms like security enclaves and TEEs. For the foreseeable future, such a system may not be feasible, but recently in Norway, BankID on mobile (BankIDpÃĕmobil) has enabled level four authentication using only a smartphone with a SIM card. BankID on mobile is however met with stark criticism by cryptographer Kristian GjÃÿsteen in the paper Protocol Variants and Electronic Identification (Gjøsteen, 2013). He provides several attack models on BankID, including the mobile version and argues that because the BankID protocol is not public and does not establish a secure channel, it cannot be considered secure. Conclusively, enabling sufficient security through only one device can prove difficult and attempting to securely enable authentication, voting and return delivery through a single device or mechanism is therefore not feasible with current technology.

Evidently, smartphones may increase availability for the electorate, but multiple challenges arise and must be addressed accordingly (Carreño et al., 2015). Unfortunately, a more detailed proposal of a smartphone voting app with the desired security features is out of scope for this project. However, introducing smartphones as an alternative method to casting votes, preferably using native apps should undoubtedly be a future consideration for governments making trials with internet voting.

Hardware Token

The University of Bern paper (Koenig et al., 2013) suggested introducing a hardware token to voters. That is a separate token delivered to voters before the election, which can be used for both two-factor authentication and return code delivery. This would however significantly reduce universality, increase cost and create administrative overhead. Because BankID on mobile now provides two factor authentication and access to level four services using one single device, has seen widespread use and is considered the most modern mechanism for signing and authentication in Norway, the current goal of BankID is to stop providing users with a physical token. This indicates that a hardware token is already considered an undesired feature of systems aiming for maximum availability and could appear like a regression to the electorate.

If however entertaining the possibility of introducing a hardware token for use in internet voting, this could be performed in combination with a national deployment. Such a token has multiple use cases in society, e.g. authentication, bank services and electronic signing. Professor Audun Jøsang and his co-workers have introduced an authentication token called the OffPAD, which goal is to be used for multiple services requiring security (Varmedal et al., 2013). They describe a physical device with a tamper proof system attempting to provide users a secure token for replacing current systems of two factor authentication. One can imagine such a device could be used for both authentications, signing votes and for the delivery of verification codes in an internet voting system. If such a device has the capabilities described and is deployed, it could eliminate using the insecure SMS channel and also enable smartphone to be used as a voting mechanism. However, the paper describing the OffPAD token is merely a proof of concept and has yet to be fully developed and prototyped.

International Framework for Internet Voting

Internet voting is performed by multiple countries using a vast array of procedures and technologies. Therefore, establishing a common international framework for internet voting could enable involved governments and companies to cooperate in the development of procedures and technologies of such systems. Currently, the only de facto standards of internet voting are the recommendations and guidelines of election experts, e.g., the Council of Europe, OSCE, the US Vote Foundation, etc.

The closest to an international standard for electronic voting is the Council of Europe's Guidelines on transparency of e-enabled elections (Stein & Wenda, 2014). These are guidelines used by more or less every state conducting internet voting. That is both because they are very definite in their explanations and requirements and because few documents regarding electronic voting are as specific and practically oriented as it is. The Council of Europe's Recommendation Rec (2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting is another document explaining both procedural, operational and technical requirements for the secure conduction of electronic voting. Because these recommendations are far more elaborate and descriptive than the other guidelines, they are consequently more difficult to adhere to.

Another significant document regarding internet voting is the OSCE handbook for New Voting Technologies (Organization for Security and Co-operation in Europe, 2013). Although a lot more extensive than the CoE guidelines, they include descriptions of democratic principles. These principles have been used extensively for the description of democracy in this project and apply to most democratic elections. Producing a common process framework for conducting internet elections would undoubtedly enable further international cooperation and sharing of experiences regarding it. However, Bull (n.d.) notes that when inspecting the different election procedures of nations, designing such a framework proves highly infeasible. There is such a vast array of different political systems and although they are mostly democratic, the processes of conduction are so different among nations that developing a set of practical guidelines is nearly impossible. Bull (n.d.) claims the only common denominator is that the counting occurs on a specific day and that even neighbouring nations as Norway and Sweden conduct elections differently. The current goal of internet voting systems should therefore still be end-to-end verifiability and following the recommendations of election experts like CoE and OSCE.

Internet Voting in Countries with Limited Trust

In nations where public trust is limited, verifiable internet voting could possibly strengthen elections. A nation with a limited degree of public trust is Uganda, which has received criticism from the European Union and the United States for its lack of transparency and detention of opposing candidates in elections. The mere suggestion of introducing internet voting in such a country is obviously controversial, but one could imagine end-to-end verifiability preserving the integrity of election results through allowing voters to verify votes. It could also possibly prevent ballot rigging, which the current president of Uganda also has been accused of (Nwokeafor, 2017).

If verifiability was implemented successfully in Ugandan election, this could strengthen trust in the integrity of election results and therefore inspire public confidence. If using repeat voting and the ability to cancel votes, internet voting could also increase equality as opposed to paper voting where voters in certain areas are violently persecuted for supporting opposing candidates to the current president, which has been in power since 1986 (Nwokeafor, 2017). End-to-end verifiability does however not prevent corrupt government leaders from denying other candidates the right to express themselves.

Although internet voting may seem like a feasible solution for such nations, the CoE guidelines state that "member states should only introduce an e-voting system if public trust in the current electoral system exists" (Maurer & Barrat, 2016). The same objective of the guidelines also states that increasing public trust should never be the single goal of introducing electronic voting. CoE bases these statements on the fact that without public and political trust, democratic principles are significantly more prone to be forfeited. Without sufficient confidence in an election or its government, internet voting is not feasible. Transparency is also an important part of building the public trust required to conduct internet elections. If the government officials responsible for conducting the election are not willing or able to disclose the details of the system and organize public consultations, it can never become a trustworthy election, regardless of voting method (Kelley, 2012).

Although internet voting can undoubtedly provide benefits like the verification of election results, such systems are also prone to errors and compromises of availability (Springall et al., 2014). Possible challenges can therefore be to provide timely election results or provide sufficient access to the voting system. In the general election of Kenya in 2007, late election results led to severe distrust resulting in riots. Problems with vote counting and reporting correct results were difficult due to multiple irregularities detected in them. The election was accused of rigging on contesting sides and according to European Union's observation, the election was flawed. The election was so controversial that citizens started rioting and chaos ensued. Consequently, if introducing internet voting in countries where public trust is low, even stronger assumptions ensure catastrophic events are not initiated or caused by faults with the internet voting system. Internet voting systems cannot enable verifiability for the detection of manipulation without also ensuring it is able to manage said manipulation accordingly.

Additionally, the economic and administrative costs of internet voting on a national scale can possibly exceed those of a paper election (Alvarez & Hall, 2003). In underdeveloped countries, the opportunity or willingness to conduct trials using internet voting may therefore be also limited by economic cost in addition to the points mentioned above.

Internet voting could possibly be used in nations where elections have been completely corrupted and has led to civil war or such extreme cases of distrust that conducting fair elections is not possible at all (Anderson & Tverdova, 2003). If an independent organization like OSCE or the United Nations could deploy internet voting, e.g. using a cloud solution, a fair election could possibly be conducted. A problem arises with promotion of candidates in such a situation. Another problem is that governments are often controlling the internet access in the country, e.g. Egypt, who during the revolution blocked internet access to multiple social media sites to prevent citizens from sharing information about the on-going change. Another issue of this suggestion is that no independent organization could take the role of election conductor for a country, as it is by the very nature of a democracy up to nations themselves to conduct their own elections. This scenario of an independent organization deploying internet voting in a country is consequently hypothetical and will probably not be considered in the foreseeable future. It is however an example of how internet voting technologies using verifiability can be used for the benefit of restoring or increasing democracy in nations where it has been reduced. Only the development of internet voting and its future implementations can reveal whether such an idealistic use of voting technologies will ever be possible (Noveck, 2009).

Blockchain

In recent years, the advancement of cryptographic currency has gained vast admiration in both the scientific community and society in general. It has not yet seen any widespread use in physical transactions, but is becoming increasingly common on the internet (CoinMarketCap, 2017). However, some of the currencies have shown great instabilities in value with both large scale frauds and major crashes already occurred several times. The most prevalent type of cryptocurrency is Bitcoin (Nakamoto, 2008), which both requires and simultaneously has enabled the technological innovation of blockchain, a public record containing and continuously recording transactions completely without the need for any central authority (Swan, 2015). The maintenance of the chain is performed through a vast communication network with nodes running software generating an increasing number of blocks in the chain.

Until recently, the most common use of blockchain technologies has been digital currency. Numerous developments have enabled blockchain to be used for other types of trans- actions, e.g. casting electronic votes. Among various companies, an entity gaining media attention is 'Follow my Vote', a non-profit organization from Virginia, who are developing an online voting platform using blockchain technologies (Lafarre et al., 2017). They claim that an internet voting system using blockchain enables sufficient transparency, integrity of election results and secrecy of votes. Although Follow My Vote's ideas are ambitious and considerate regarding democratic principles, they have yet to present a complete implementation. Only when more accurate specifications of the system are provided can it be investigated whether such a system is suitable for future governmental elections. Additionally, governments and election officials need to gain more knowledge and familiarity with such technologies before attempting to introduce them to current voting systems.

Currently, communication seems to be limited between the scientific communities involved with blockchain and those with internet voting. An inspection of various blockchain voting proposed systems suggest that those involved in blockchain does not yet sufficiently understand all the challenges of internet voting, indicated by multiple blockchain voting systems discussing anonymous voting as a key feature. It is not evident whether these entities actually mean anonymous voting, or whether they are confusing the terminology with secret voting. Either way, anonymity has never been a desired feature of any democratic system and the secrecy of votes does not involve voters being anonymous, but that their choice is never revealed. Additionally, current blockchain technologies do not provide complete anonymity, but rather pseudonymity. That means they are able to mask the origin of transactions by linking owner identity to a certain pseudonym. This can be considered disadvantageous for voting systems, which require complete voter privacy. A final note must be made regarding the fact that very few significant election entities with the exception of the US Vote Foundation has yet started discussing the possibilities of using blockchain technologies for voting (Murray et al., 2015).

However, Ukraine has recently displayed interest in trailing an election platform based on a blockchain technology called Ethereum (Manski, 2017). This technology uses a property called smart contracts, a protocol that enables a transaction to be enforced with verification. The system will be implemented by a company called Ambisafe using the product e-vox. Although their website does not reveal whether this system will be end-to-end verifiable, one can imagine that Ukraine, a nation severely set back by its political uprising and allegations of voter fraud in recent years is able to benefit from such a system either way. It will be interesting to see to what extent the system is able to provide transparency and inspire public confidence.

Conclusions

All elections, including those enabling the use of the internet to cast votes must retain democratic principles. These principles aim to protect the secrecy of votes and preserve the integrity of election results in a transparent manner. Only if an election can sufficiently retain these principles, it can be considered democratic and internet voting has the potential to increase the confidence in enforcement of these principles. Some of the ideas and mitigating features are suggested, e.g., introducing a hardware token, should be considered for future improvements to the voting system. A suggestion to use blockchain technologies for the conduction of internet voting is also proposed. Blockchain is however a very recent and somewhat immature technology. Nor do election experts display any significant interest in such developments. However, Ukraine has very recently decided to conduct election trials using blockchain technologies.

References

Al-helali, M. A. S., & Hameed, W. W. A. (2010). A secure electronic voting. Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements: E-Government Strategies and Advancements, 431.

Alvarez, R. M., & Hall, T. E. (2003). *Point, click, and vote: The future of internet voting*. Brookings Institution Press.

Anderson, C. J., & Tverdova, Y. V. (2003). Corruption, political allegiances, and attitudes toward government in contemporary democracies. *American Journal of Political Science*, 47 (1), 91– 109.

Anderson, R. (2008). *Security engineering*. John Wiley & Sons.

Bellovin, S. M. (1989). Security problems in the tcp/ip protocol suite. *ACM SIGCOMM Computer Communication Review*, 19 (2), 32–48.

Broache, A. (2016). Estonia pulls off nationwide net voting. CNET News.

Bull, C. (n.d.). Unstructured Interview with Christian Bull. Norwegian Personal Communication.

Carreño, P., Gutierrez, F. J., Ochoa, S. F., & Fortino, G. (2015). Supporting personal security using participatory sensing. *Concurrency and Computation: Practice and Experience*, 27 (10), 2531– 2546.

CoinMarketCap. (2017). Crypto-currency market capitalizations. http://coinmarketcap.com.

Cranor, L. F., & Cytron, R. K. (1997). Sensus: A security-conscious electronic polling system for the internet. In Proceedings of the thirtieth hawaii international conference on system sciences (Vol. 3, pp. 561–570).

De Faveri, C., Moreira, A., Araújo, J., & Amaral, V. (2016). Towards security modeling of e-voting systems. In 2016 ieee 24th international requirements engineering conference workshops (rew) (pp. 145–154).

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, 239-288.

Diakopoulos, N. (2015). Algorithmic accountability: Journalistic investigation of computational power structures. *Digital journalism*, 3 (3), 398–415.

Feroze, A., & Basharat, A. (2011). Security analysis of mobile banking services in Pakistan. *Asian Transactions on Fundamentals of Electronics, Communication & Multimedia*, 1 (3), 13–17.

Department for Communities & Local Government. (2006). Strong and prosperous communities: The local government white paper (Vol. 6939). The Stationery Office.

Organization for Security and Co-operation in Europe. (2013). Handbook for the Observation of New Voting Technologies.

Gjøsteen, K. (2013). Protocol variants and electronic identification. *IACR Cryptology* ePrint Archive, 329.

Gritzalis, D. A. (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, 21 (6), 539–556.

Habermas, J. (1994). Three normative models of democracy. *Constellations*, 1 (1), 1–10.

Hao, F., & Ryan, P. Y. (2016). Real-world electronic voting: Design, analysis and deployment. CRC Press.

Harwood, M. (2010). *Security strategies in web applications and social networking*. Jones & Bartlett Publishers.

Heiberg, S., & Willemson, J. (2014). Verifiable internet voting in Estonia. In 2014 6th international conference on electronic voting: Verifying the vote (evote) (pp. 1–8).

Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004). A security analysis of the secure electronic registration and voting experiment (serve). New York Times (http://www. servese- curityreport. org).

Jensen, C. D. (2014). The importance of trust in computer security. In international conference on trust management (pp. 1–12).

Kelley, J. G. (2012). *Monitoring democracy: When international election observation works, and why it often fails*. Princeton University Press.

Koenig, R. E., Locher, P., & Haenni, R. (2013). Attacking the verification code mechanism in the norwegian internet voting system. In International conference on e-voting and identity (pp. 76–92).

Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. In Ieee symposium on security and privacy, 2004. proceedings. 2004 (pp. 27–40).

Lafarre, A., et al. (2017). Blockchain and the 21st century annual general meeting. European Company Law, 14 (4), 167–176.

Manski, S. (2017). Building the blockchain world: Technological commonwealth or just more of the same?. *Strategic Change*, 26 (5), 511–522.

Marias, G. F., Barros, J., Fiedler, M., Fischer, A., Hauff, H., Herkenhoener, R., . . . others (2012). Security and privacy issues for the network of the future. *Security and Communication Net- works*, 5 (9), 987–1005.

Marsh, S., & Dibben, M. R. (2003). The role of trust in information science and technology. *Annual Review of Information Science and Technology*, 37 (1), 465–498.

Maurer, A. D., & Barrat, J. (2016). *E-voting case law: a comparative analysis*. Routledge.

McGaley, M., & McCarthy, J. (2004). Transparency and e-voting: Democratic vs. commercial interests. *Electronic Voting in Europe*, 47 , 153–163.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

Meter, C. (2017). Design of distributed voting systems. arXiv preprint arXiv:1702.02566.

Moynihan, D. P. (2004). Building secure elections: e-voting, security, and systems theory. *Public administration review*, 64 (5), 515–528.

Murray, J., Kiniry, J., Zimmerman, D., & Dzieduszycka-Suinat, S. (2015). The future of voting: End-to-end verifiable internet voting specification and feasibility.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Noveck, B. S. (2009). Wiki government: how technology can make government better, democracy stronger, and citizens more powerful. Brookings Institution Press.

Nwokeafor, C. U. (2017). Chapter of the history of election and the integration of technology in the electoral process: A review of Uganda's 2016 election outcome.

Technology Integration and Transformation of Elections in Africa: An Evolving Modality, 178.

Oostveen, A.-M., & Van den Besselaar, P. (2004). Security as belief: users' perceptions on the security of electronic voting systems. *Electronic voting in Europe: Technology, law, politics and society*, 47, 73–82.

Rakodi, C. (2003). Politics and performance: the implications of emerging governance arrangements for urban management approaches and information systems. *Habitat international*, 27 (4), 523–547.

Ramchurn, S. D., Huynh, D., & Jennings, N. R. (2004). Trust in multi-agent systems. *The Knowledge Engineering Review*, 19 (1), 1–25.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman,J. A. (2014). Security analysis of the Estonian internet voting system. In Proceedings of the 2014 acm sigsac conference on computer and communications security (pp. 703–715).

Starr, A., Al-Najjar, B., Holmberg, K., Jantunen, E., Bellew, J., & Albarbar, A. (2010). Maintenance today and future trends. In E-maintenance (pp. 5–37). Springer.

Stein, R., & Wenda, G. (2014, October). The Council of Europe and e-voting: History and impact of Rec (2004) 11. In *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)* (pp. 1-6). IEEE.

Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

Sztompka, P. (1999). Trust: A sociological theory. Cambridge University Press.

Tkacheva, O. (2013). Internet freedom and political space. Rand Corporation.

Varmedal, K. A., Klevjer, H., Hovlandsvåg, J., Jøsang, A., Vincent, J., & Miralabé, L. (2013). The offpad: Requirements and usage. In International conference on network and system security (pp. 80–93).

Vasudevan, A., Owusu, E., Zhou, Z., Newsome, J., & McCune, J. M. (2012). Trustworthy execution on mobile devices: What security properties can my mobile platform give me? In International conference on trust and trustworthy computing (pp. 159–178).

Wagner, D., Jefferson, D., Bishop, M., Karlof, C., & Sastry, N. (2006). Security analysis of the diebold accu basic interpreter (Tech. Rep.).

Wardman, B. (2011). A series of methods for the systematic reduction of phishing. The University of Alabama at Birmingham.

Wenda, G., & Krimmer, R. (2016). Towards an update: The council of europeï£¡s ad-hoc com- mittee of experts on e-voting (cahve) and its impact on international organisations1. In the Ipsa conference, poznan.

Wollscheid, S., & Hammerstrøm, K. (2012). Effekt av tiltak for å lette livsoverganger for barn og unge med funksjonsnedsettelser. Rapport fra Kunnskapssenteret.

Wright, J. (1996). The osce and the protection of minority rights. Hum. Rts. Q., 18 , 190.