ANALYSIS OF ELECTRONIC VOTING SCHEMES IN THE REAL WORLD

Voke Augoye, Allan Tomlinson
Information Security Group, Royal Holloway, University of London.
Egham, Surrey. TW20 0EX, UK
Email: voke.augoye.2011@live.rhul.ac.uk, allan.tomlinson@rhul.ac.uk

Abstract

Voting is at the heart of a country's democracy. Assurance in the integrity of the electoral process is pivotal for voters to have any trust in the system. Often, electronic voting schemes proposed in the literature, or even implemented in real world elections do not always consider all issues that may exist in the environment in which they might be deployed.
In this paper, we identify some real-world issues and threats to electronic voting schemes. We then use the threats we have identified to present an analysis of schemes recently used in Australia and Estonia and present recommendations to mitigate threats to such schemes when deployed in an untrustworthy environment.

Keywords: Insider Threat, Authentication, Cyber Threat, Electoral Fraud, Privacy, Trust

1 Introduction

As democracies continue to grow, citizens of a lot of nations, more so in the developing countries, are beginning to clamour for the introduction of electronic voting because they believe the traditional paper based systems are often marred by wide scale electoral fraud (Jensen & Justesen, 2014; Dominguez & James, 1998; Lehoucq, 2003; Craig & Cornelius, 1995; Heskey & Bowler, 2005)

One common issue with e-voting schemes is that the environment assumed during design may not fully consider the threats that exist in real world deployment. Thus, when these schemes are deployed some vulnerabilities may appear that were not considered in the initial threat model.

The voting *environment* and how voting schemes relate to other parts of the voting process goes a long way in determining which security requirements are necessary and which requirements may be satisfied by default. For example, a remote voting scheme and a supervised in-person voting scheme are two different voting environments and provide different levels of security by default. A supervised voting scheme can provide coercion resistance by being supervised but remote voting schemes do not give such guarantees by

default. Consequently, remote voting schemes need to rely on technical security provided by cryptography.

With electronic voting, voter authentication is an open issue; it can be quite complicated authenticating the voter if done remotely. For example, a spouse may vote on behalf of her partner and there is no way the system can tell the difference. Some e-voting schemes have tried to address this threat by using smartcards (Abandah, Darabkh, Ammari, & Qunsul, 2014; Springall, et al., 2014) as an instance of the voter. If the smartcard is authenticated as done in the Internet voting scheme used in Estonia (Springall, et al., 2014) then the voter is assumed to have been authenticated correctly.

Many voting schemes might work in one environment but might not work in another because of socio-economic factors (such as religion, poverty). These factors may determine how effective the voting schemes would be in such environments. For example, in a world where no one wants to cheat the system, we wouldn't have to worry about voters being coerced or ballot stuffing.

It is well known that a system is only as secure as the weakest component. In a remote voting environment, while the network and servers are secure, there is no assurance that voter's computers are secure. In the Estonian I-voting scheme, voter's computers were assumed to be secure. Subsequently, in a mock election (Springall, et al., 2014), a group of researchers were able to attack voters' computers and change votes to their choice. So, to have assurance that the entire voting scheme is secure, the voter's computer needs to be secure as well.

Another common assumption made, is the trust placed on electoral officials. In precinct voting schemes, we trust electoral officials to correctly authenticate voters and prevent double voting (Culnane, Ryan, Steve, & Vanessa, 2015). However, this is not always the case in real world elections where the electoral officials may be part of the fraud (Asunka, Brierley, Golden, Kramon, & Ofosu, 2013).

Hence, to build a secure e-voting scheme, security must be considered at the outset and designed into the system. Security of all software and hardware should be analysed and proved secure if possible, however the level of security also depends on the environment where it is deployed.

In this paper, we identify the security requirements for an e-voting scheme in section 2 and in section 3 we analyse threats that exist in the real world. In section 4 we review two well known voting schemes, the I-voting scheme used in Estonia and the prêt-a-voter scheme used

in Australia, presenting a security analysis of each. We discuss the analysis in section 5 and present our conclusions in section 6.

2 Security Requirements of an Electronic Voting Scheme

Electronic voting is more complicated than other electronic transactions such as e-commerce. Many of the security requirements required for an electronic voting scheme are not necessarily needed in other electronic transactions. Moreover, electronic voting has conflicting security requirements which are difficult to resolve, for example verifiability and receipt-freeness (Chevallier-Mames, Fouque P, Pointcheval, Stern, & Traoré, 2010)

Most security requirements for e-voting also apply to traditional paper based voting. However, *universal verifiability* is not satisfied in traditional paper based schemes. Based on an analysis of the literature (Schoenmakers, 1999; Delaune, Kremer, & Ryan, 2006; Jan, Chen, & Lin, 2001; Karr & Wang, 1999; Fujioka, Okamoto, & Ohta, 1993; Benaloh & Tuinstra, 1994; Cramer, Franklin, Schoenmakers, & Yung, 1996; Anane, Freeland, & Theodoropoulos, 2007; Burmester & Magkos, 2003) the following describes what we believe should be the main security requirements an electronic voting scheme.

- **Coercion Resistance**: a coercion resistant scheme prevents a coercer from forcing voters to reveal their ballot.
- **Receipt freeness**: this property ensures that a voter doesn't get any information that could be used to prove to anyone how he voted. This requirement helps to check vote buying and selling.
- **Individual verifiability**: this property implies that a voter is able to confirm that their vote was cast as intended.
- **Universal Verifiability**: in a universal verifiable scheme, *anyone* can confirm that votes have been recorded as cast and counted as cast.
- **Privacy**: This requires that the identity of the voter is not revealed. Thus, from a vote cast, it should be impossible to identify the voter. This is closely linked with, but different from, anonymity which is the unlinkability between the voter's identity and the vote cast. This requirement gives e-voting the ballot secrecy achieved using ballot boxes in traditional paper based elections.

- **Democracy**: An electronic voting scheme should ensure only eligible voters can vote and they cannot cast multiple votes.
- **Robustness**: A robust scheme should be resilient to external attacks such as denial of service attacks; should prevent inclusion of votes by corrupt parties for abstained voters; and should be able to recover from any faulty behavior due to collusion by malicious parties.

2.1 Types of Electronic Voting

Electronic voting is the communication of votes by electronic means using electronic devices. Voting can either be done remotely via the Internet (Internet Voting) or by using a voting machine at a precinct which is usually referred to as supervised voting scheme.

Supervised e-voting schemes are like traditional voting schemes because they make use of voting kiosks and are supervised by polling officials. If voting is done remotely or in a voting kiosk, it could determine the security requirements satisfied by default. In a supervised environment, polling officers are meant to prevent coercion of voters. In a remote setup, schemes try to provide coercion resistance by allowing *re-voting* as seen in the I-voting in Estonia (Springall, et al., 2014). This allows voters to vote manually which supersedes an electronic vote (Springall, et al., 2014) and overrides the use of credentials/votes used by a coercer (Clarkson, Chong, & Myers, 2008).

3 Threat Analysis in Real World Voting Schemes

In this section, we consider issues that may affect the integrity of elections in real world implementations if not included during the design phase of e-voting schemes.

3.1 Socio-economic Issues

It has been documented that vote buying and vote selling is very prevalent in real world electronic voting. In Mexico, voters were so suspicious about the integrity of elections because of the electoral fraud committed by parties (Dominguez & James, 1998). Such fraud relied on many techniques including ballot stuffing by both voters and electoral officials; stealing of ballot boxes between the polling units and collation centres; intimidation of voters, observers and party officials; and manipulating voter's registration lists (Ferree, Gibson, &

Long, 2014; Asunka, Brierley, Golden, Kramon, & Ofosu, 2013; Craig & Cornelius, 1995; Heskey & Bowler, 2005).

Vote buying, selling and coercion is common practice in elections. In an analysis done in Taiwan (Nichter S. , 2014) as little as $10 was paid to voters to sell their votes. This is not surprising because of the economic situation in many countries, and vote buyers usually target poor voters. In the USA five Democratic Party Operatives were convicted in a federal court in 2004 for offering poor people cigarettes, medicine, beer and $5 to $10 dollars for their votes (Nichter S. , 2008).

In other cases, electoral officials are part of this electoral fraud. A report about the 2012 elections in Ghana recorded issues like double voting, under age voting, over voting and voting by ineligible individuals (Asunka, Brierley, Golden, Kramon, & Ofosu, 2013). This was possible because the poll-site officials were trusted to prevent this. These issues are difficult to address solely by human supervision because the trusted polling officials are sometimes part of the fraud, usually for financial gain.

Voting schemes cannot prevent all forms of electoral fraud since there is always a financial incentive to cheat the system due to socio-economic challenges. However, design of voting schemes should take these threats into account and leverage on technical security wherever possible to ensure that any deliberate attempt to circumvent the technology is detected.

3.2 Insider Threat

According to (Schneier, 2009) “Insiders are especially pernicious attackers because they're trusted. They have access because they're supposed to have access. They have opportunity, and an understanding of the system, because they use it or they designed, built, or installed it. They're already inside the security system, making them much harder to defend against.”

The UK Cyber strategy also notes that “Computer systems, networks and applications all rely upon people for their development, delivery, operation and protection and the likely success of an attack is increased when a so-called ‘insider’ is involved” (Cabinet Office, 2009).

The insider threat is a well-documented issue and one of the biggest threats to organizations. About 53% of attacks on organization have been deliberate actions or negligence by staff. 54% of IT staff feel it is difficult to detect insider threats while 33% of organization have no formal response plan (Cole, 2014).

Attackers have realized that it is difficult to attack secure networks, so they find easier routes, like targeting individuals that work in organizations. An example is the 2011 attack on RSA secureID where phishing emails with an attachment that contained malware was sent to a group of unsuspecting employees who downloaded the files allowing the attackers to gain access to the network[1].

In e-voting literature, the insider threat and how it could mar an election is not often considered. Instead some schemes assume electoral officials can be trusted to carry out vital functions such as authentication (Springall, et al., 2014) of voters or transfer of sensitive information from one entity (i.e. a server) to another (Culnane, Ryan, Steve, & Vanessa, 2015). This could have been done more securely by technology. This trust in human procedures and processes over technology is an assumption in the I-voting scheme and prêt-a-voter.

In an analysis of the electoral process in Estonia (Springall, et al., 2014), researchers recorded various lapses in procedures which introduced vulnerabilities that could be exploited. The financial benefits for malicious insiders is enough incentive for them to either aid an attack or look the other way when this happens.

With vulnerable electoral officials, it is important to ensure that the technical security employed in voting schemes should reduce threats posed by insiders. Hence, auditability of the process and verifiability of votes cast should be satisfied for a voting scheme to be credible.

In section 4 we do an analysis of the vVote: a verifiable voting scheme (Prêt-a-voter) and I-voting scheme to shed more light on this issue.

3.3 Cyberthreat and Foreign Government Influence

Cyber threat and cyber warfare has become a serious issue that organizations and governments are dealing with. There have been various reported cases of state sponsored attacks like the alleged North Korean attack on Sony[2] or alleged United States attack on Iranian nuclear enrichment plant (Langner, 2001). Increasingly we continue to see allegations of foreign government influence in the democratic processes of other nations.

---

[1] http://www.eweek.com/c/a/Security/RSAs-SecurID-Breach-Started-with-Phishing-Email-318649

[2] http://www.ft.com/cms/s/0/287beee4-96a2-11e4-a83c-00144feabdc0.html#axzz3h4p5qypf

In addition to the current controversy surrounding recent elections in the USA, it has been alleged that Russia carried out a state sponsored Distributed Denial of Service (DDoS) attack on Estonia in 2007[3]. In Hong Kong, the largest and most sophisticated ever DDoS attack hit an online democracy poll that canvassed opinions for future elections in the country[4]. Also, in Ukraine a virus that was meant to delete votes during the presidential elections hit their Central Election Authority[5].

In Washington DC, an Internet voting system was designed to allow oversea absentee voters cast their votes, this was a pilot project and it was tested as a mock election in 2010. Some researchers (Wolchok, Wustrow, Isabel, & Halderman, 2012) attacked this system and gained full access within 48 hours, changing every vote and revealing almost all secret ballots.

These Cyber-attacks have created a completely different threat environment that did not exist before, and now that nations are pushing for e-voting this should be considered when designing e-voting schemes.

In the literature, many schemes don't consider the threat of a cyber-attack. In the I-voting scheme used in Estonia, lapses where shown in the electoral process and architecture that could create avenue for a cyber-attack (Springall, et al., 2014). The implicit trust placed on voters' computers in some Internet voting schemes clearly shows that cyber threat was not considered in their design.

3.4 Threat Model

Based on the review in the previous section and sections 4.3 and 4.4 we present a threat model in Table 1 and make some assumptions about the attacker. We do not consider *all* the threats that exist in e-voting, only threats we believe are most important.

Threat	Vulnerability	Impact	Scheme
Poll-site officials	Trust placed on poll-site officials to authenticate voters using traditional	Votes are cast for abstained voters without being detected by the	Pret-a-voter

[3] http://www.theguardian.com/world/2007/may/17/topstories3.russia

[4] http://www.theregister.co.uk/2014/06/23/most_sophisticated_ddos_strikes_hk_democracy_poll/

[5] http://www.rt.com/news/161332-ukraine-president-election-virus/

vote on behalf of abstained voters.	means as used in paper based elections. Ballots are not authenticated hence not digitally linked to voter.	system and could change the outcome of the election.	
An attacker can stuff the ballot without being detected.	Ballots are not digitally linked to voter.	Double voting by legitimate voters. Ballot stuffing by poll-site officials without being detected and could change the election outcome.	Pret-a-voter
Poll-site officials can allow ineligible voting	Trust placed on officials over technical means to authenticate (i.e Biometrics) voter.	Ineligible people can cast ballots undetected by the system, compromising election integrity	Pret-a-voter
An attacker can install a vote altering or data stealing malware in election servers and voter's computers.	Unclean computers used to prepare voting client software sent to voters.	Attacker alters votes to that of his choosing without being detected. Spyware monitors how voters voted, breaking ballot secrecy and could enforce voter coercion.	I-Voting
Vote selling to coercers by voters.	Trust placed on voter to tear candidate list that links ballot to voter.	Voter can leave poll-site with candidate list and show a third party there by breaking privacy, receipt-freeness and coercion resistance.	Pret-a-voter

Denial of Service Attacks	Improper input validation.	Disruption of electoral process and hence disenfranchising legitimate voters.	I-voting

Table 1. Threat Model

3.4.1 Capability of the Attacker

In this section, we make some assumptions about the attacker based on our threat model

- An attacker can either be an insider or an outsider.
- An attacker may be motivated by financial incentives to cheat the electoral process.
- A voter may be motivated by financial incentives to cheat the electoral process
- We assume that an attacker has the following capabilities:
  1. An attacker can stuff the ballot box without being detected.
  2. An attacker can vote on behalf of an abstained voter or allow ineligible voting.
  3. An attacker has adequate resources to carry out a DDoS attack
  4. An attacker can tell the link between a voter's id and the cast ballot.
  5. An attacker can install vote altering, or data stealing malware in election servers and voters' computers.

4 Electronic Voting Scheme

In the previous section we identified threats to e-voting schemes in the real world. In this section, we now review two electronic voting schemes in the light of the threats and requirements discussed earlier.

4.1 vVote: A Voter Verifiable Voting Scheme (Prêt-a-voter)

The prêt-a-voter voting scheme is an end-to-end verifiable scheme that provides privacy. It uses a candidate list which is printed on demand before voting. This candidate list has the names of candidates arranged in a random order. The voter can audit this candidate list to confirm that it has the correct encryption of the random arrangement of the candidates. If this audit is done, the candidate list is decrypted and hence cannot be used to cast a vote to maintain the secrecy of the ballot (Burton, Culnane, & Schneider, 2015). A QR code of the candidate list is scanned into a tablet and this launches the vote capture application. The voter

fills the ballot using the tablet. After completing the ballot, a preference receipt (PR) is printed. The voter can compare the candidate list with the preference receipt to confirm that they are both arranged in the same order, this gives the voter assurance that his vote has been cast as intended. The candidate list is expected to be destroyed after confirmation, to maintain ballot secrecy while the preference receipt is kept by the voter. At the end of the elections, a voter uses the preference receipt to confirm that his vote has been published on a Web bulletin board at the final tally. This gives voters assurance that their votes have been recorded as cast (Burton, Culnane, & Schneider, 2015). Further details could be found in the draft report (Culnane, Ryan, Steve, & Vanessa, 2015)

4.2 Estonia Internet Voting System (I-voting)

Over 30% of votes cast in elections done in Estonia today are done electronically this makes Estonia one of the front runners in the use of electronic voting for elections and the first country to use Internet voting nationally (Springall, et al., 2014). Estonia has a national ID card which has cryptographic keys issued by the government which are used to authenticate voters during election. The scheme attempts to replicate the double envelope process used in postal voting. A digital signature is generated with the voter's signing key and this is used to provide the voter's identity (outer envelope). The system's public encryption key is used to encrypt the ballot to provide secrecy (the inner envelope). The signature is stripped from the ballot leaving a set of anonymous encrypted votes once the eligibility of all voters has been established. These anonymous votes are then transferred to a physically separate vote counting server connected to a hardware security module for decryption.

The Estonian voting system uses a *vote forwarding server* which is the only publicly accessible server. This server communicates with the client software and forwards vote to a *vote storage server*. Votes are copied using DVDs to the *vote counting server* by electoral officials. The vote counting server is not connected to any server. The Estonian Internet voting system is not end-to-end verifiable and much of security it provides relies on human procedures rather than technical means thereby placing lot of trust on electoral officials. Further details about how this voting scheme really works can be found in (Heiberg & Willemson, 2014, Springall, et al., 2014).

4.3 Security Analysis of vVote: A Verifiable Voting Scheme (Prêt-a-voter)

Prêt-a-voter, used in Australia, relies on traditional means to validate eligibility (Democracy see section 2). If this scheme is to be adopted in other environments, this may not work since part of the reason why nations clamour for electronic voting is the inadequacies of traditional means of authenticating voters. As stated in our threat model, relying on poll-site officials to authenticate voters could leave the system vulnerable to ineligible voting. This risk could be mitigated using Photo ID but cannot be eliminated by this approach alone especially if the polling officials are untrustworthy.

This scheme expects voters to destroy the human readable candidate's list after casting their votes, this puts a huge level of trust on voters to do this. Privacy is an important requirement of e-voting as well as receipt freeness which helps to mitigate vote buying, vote selling and voter coercion. If voters fail to destroy this human readable part, which isn't unthinkable considering the socio-economic challenges (Section 3.1), then this scheme would not provide privacy. Because with this candidate list you can make a link between the candidates and vote cast published on the bulletin board as highlighted in our threat model is section 3.4.

Furthermore, with the candidate list, voters have proof to show a vote buyer or a coercer. Thus, this scheme would fail to provide coercion resistance (section 2) and gives voters the opportunity to sell their votes to vote buyers.

Ballot stuffing, double voting and voting in place of abstained voters could go a long way in determining who wins an election and has been reported in several elections, an example is the 2012 national elections held in Ghana (Asunka, Brierley, Golden, Kramon, & Ofosu, 2013).

The prêt-a-voter scheme is as vulnerable to corrupt official as traditional schemes and this needs to be mitigated using technical means. A corrupt official could vote for an abstaining voter and this wouldn't be detected by the system because of unlinkability between voter and the ballot cast; and lack of technical means for authentication. Schemes like the I-voting in Estonia solve this problem by using a smartcard which is an instance of the voter. This link prevents corrupt officials from voting for abstained voters without physically having their smartcards. Prêt-a-voter system is meant to be end-to-end verifiable but the attacks mentioned cannot be detected by the system and represent a big risk to take in certain environments. Hence, considering insider threats and socio-economic issues like poverty, prêt-a-voter may not offer any better security than traditional schemes.

However, prêt-a-voter would improve efficiency and minimize human errors in the vote counting process and if we could guarantee that the electoral officials and voters are trustworthy then it may well satisfy its security claims but this is easier said than done in the real world.

In conclusion, prêt-a-voter is vulnerable to breach of privacy, vote buying and selling since achieving receipt-freeness relies on voters being trustworthy, ballot stuffing, ineligible voting is possible if trust assumptions are broken.

4.4 Analysis of Estonian Internet Voting Scheme

A group of researchers observed the Estonian elections and produced a report which showed lapses in the electoral process that could undermine the integrity of the election. One of the issues raised was the use of procedural means over more technical means to provide security. A high degree of trust, as seen in prêt-a-voter system, was placed on electoral officials, making security critical aspects of the system rely on, sometimes, a single individual. Trust was also placed on the integrity of voters' computers as well as the various servers used. We will consider some of these lapses to support our argument but a full report on this election can be found in (Springall, et al., 2014).

Contrary to security best practices electoral officials logged on to servers using root access. This is a major lapse because the system cannot tell which official accessed it. This creates an opportunity for a malicious insider to carry out attacks such as installing malware that could alter votes between decryption and tabulation, or stealing information that could compromise vote privacy as highlighted in our threat model in section 3.4

It was also observed that the vote storage server reported an error suggesting that the drive configuration had changed when it was booting during the tabulation phase. Instead of the officials investigating this error, it was simply bypassed in this critical phase of the election where encrypted votes are exported. In other instances, servers were simply rebooted to clear error messages rather than troubleshooting. If these errors were caused by malware, the officials would not have noticed. And since the system is not end-to-end verifiable, voters and auditors cannot tell if votes are counted as cast in the final tally.

It was also documented that officials downloaded client software using an unsecure http connection. This makes the system vulnerable to a network man-in-the-middle attack which could compromise the election. Unclean laptops that had links to gambling sites and bit

torrents installed were used to prepare client software distributed to the public, this could introduce malware into voter's computers (section 3.4) on a large scale. Most attacks on organizations are carried out because unsuspecting insiders are targets of cyber attackers. So even if the electoral officials are not genuinely part of the electoral fraud, their actions as have just been highlighted leaves the electoral process vulnerable to attacks.

In the Estonian system, a voter can verify with an application (Springall, et al., 2014) that their vote was cast as intended. However, with the increasing interaction between smart phones and computers it is not difficult to imagine that both devices can be corrupted making it difficult for the voter to notice that their votes have been altered.

In the tabulation phase, it was also reported that a technical glitch occurred and an official's personal flash drive, that contained other personal files, was used to copy unencrypted votes to a laptop connected to the internet where the official result was signed. If this USB contained malware, this would mean the votes could have been altered without detection. Furthermore, the flash drive could have introduced malware to the counting server, this malware could be a spyware which could have the ability to monitor the decryption process and hence know the relationship between a voter and a ballot- breaching voter's privacy. These possibilities were identified in our threat model in section 3.4.

From the published portions of the I-voting server software the researchers found out that the log server, which logs information from the vote forwarding and vote storage servers, saved any unexpected data to disk. If this storage gets exhausted voting would stop allowing a denial of service attack Such an attack is well within the means of the state sponsored attacker or even a modest attacker with adequate resources (section 3.4) depending on the size of the disk. Furthermore, storing of unexpected data means the system is vulnerable to other attacks.

In conclusion, we can see that this scheme is vulnerable to many attacks such as DDoS, breach of privacy, and vote alteration. Some of these attacks are possible because the scheme is not universally verifiable (section 2) and trust was placed on human procedures and processes rather than technical security.

5 Discussion

It is clear that while existing e-voting schemes may be secure in benign environments, their adoption for use in untrustworthy environments presents a number of risks. In section 3, we

identified the threats to e-voting schemes and how these could impact security. In this section, we do a further analysis on the schemes considered in section 4, highlighting the motivation for the attacker, vulnerabilities that could be exploited and some ways to mitigate the threats.

Authentication: In the prêt-a-voter scheme, we have shown that trust placed on electoral officials may allow ineligible voters vote, over voting and voting on behalf of abstained voters. These vulnerabilities could be prevented by the introduction of a tamper-resistant token, such as a smartcard which is difficult to clone. With smartcards voters can be authenticated correctly preventing ineligible voters from voting. Such a device could also sign ballots ensuring linkability between the voter's id and cast ballot. Linkability would ensure officials cannot vote for absent voters without the smartcard in their possession, preventing ballot stuffing.

However, the use of smartcards comes at an extra cost and the added advantage of introducing a smartcard may not be justified. The Estonian National ID card which has cryptographic keys for both authentication and digital signature adequately addresses the issue of ballot stuffing and voter's authentication. There also exist other electronic voting schemes that use smartcards for authentication of voters (Langner, 2001), prevention of double voting and impersonation of abstained voters (Abandah, Darabkh, Ammari, & Qunsul, 2014).

Incentives: In the prêt-a-voter scheme, the trust placed on voters creates an opportunity for vote buying, vote selling and coercion because of the possibility of voters carrying the human readable candidate list out of the polling booths. This means receipt-freeness, which underpins privacy and coercion-resistance, relies on voters who may not always be trustworthy. We have shown that considering the socio-economic issues in societies, there is an incentive for voters and electoral officials to partake in corrupt electoral practices. In many environments, a voting system cannot rely solely on trustworthy voters or electoral officials but should rather rely on technical measures for security sensitive processes.

In the I-voting scheme, the procedural lapses highlighted in section 4.4 creates an avenue for a malicious insider to infect voter's computers on a large scale. Personal devices should not

be used to prepare client software sent to voters. Special purpose laptops or PCs dedicated to this task should be used. Moreover, the integrity of any software should be checked at intervals to ensure that the client software has not been tampered with.

Verifiability: The I-voting scheme places trust on the voter's client machine. Malware can be introduced to the system by taking advantage of procedural lapses highlighted in section 4.4 above. This kind of attack would go unnoticed by voters and auditors because the scheme is not end-to-end verifiable (verifiability section 2). Trust was placed on the voter's client machine, human process and procedures to prevent this. Our argument is that such trust is misplaced, thus verifiability is difficult to guarantee.

Further attacks on the I-voting system were carried out on both the client side and server side affecting ballot secrecy and voter's privacy (Springall, et al., 2014). The prêt-a-voter scheme, however, is end-to-end verifiable from vote casting to the final count and tallying of results. Any vote alteration would be detected both by voters and third parties because this scheme relies on sound security practices to provide verifiability rather than relying on human processes and procedures.

Cyber Attacks: We have shown that Cyber-attacks by well-resourced attackers or state sponsored attackers are a threat to electronic voting which did not exist in traditional paper based schemes. The DoS attack that could stop voting in the I-voting scheme by exploiting data logging (see section 4.4) can be prevented by ensuring proper validation of input data. Furthermore, the use of unclean laptops to prepare client software sent out to voters creates an avenue for wide scale malware infection of voters' computers. This kind of vulnerability could leave the entire e-voting process vulnerable to a full scale cyber-attack. In the pret-a-voter scheme the voting is done in a more controlled environment since elections are done in a precinct and all the equipment used are under the control of the electoral authorities.

Technical Security vs Human Procedures and Processes: Many technical solutions to ID verification rely on PINs or passwords. These may be stolen, or shared. Alternatively, a physical token could be issued that generates temporary passwords or PINs. This gives an extra level of security because even if PINs have been compromised an attacker would still require a physical token to make use of that information. We argue that the cost of issuing

such tokens may be justified depending on the environment where the e-voting scheme is deployed.

We have shown from both schemes analysed, that the part of the scheme where technical means are used to provide security and the kind of trust assumptions made could determine which security requirements would be satisfied. In the prêt-a-voter scheme, from vote casting to the final vote tallying is end-to-end verifiable but the Estonian Internet Voting scheme is not.

This gap in technical verifiability between authentication and vote casting in prêt-a-voter, and in the I-voting scheme between vote casting and vote tallying, introduces weakness which could be exploited by an attacker as discussed in sections 4.3 and 4.4.

In the prêt-a-voter scheme authentication was undertaken by traditional means since it is a supervised scheme, this is a sharp contrast from the I-voting scheme which used a smartcard to authenticate voters. The lack of technical authentication in pret-a-voter creates the opportunity for electoral officials to cheat the system as discussed in section 4.3 without being detected.

On the other hand, the trust placed on voters to destroy the human readable part of the prêt-a-voter ballot form used to verify votes are cast as intended, creates another vulnerability that could be exploited by voters to break ballot secrecy and sell votes. In the I-voting scheme, a verification app on a smart phone is used to check that votes have been cast as intended. However, in this scheme, a coercer can watch a voter while voting. This could be mitigated by a re-voting option to override any coerced vote. In cases where the voter is corrupt, no technology can prevent the voter from selling votes or allowing someone vote in his stead because this scheme is not supervised.

In conclusion, both e-voting schemes reviewed have advantages and disadvantages in terms of meeting the requirements for a secure e-voting scheme. However, neither scheme is able to meet all requirements. In particular, we have identified two issues that need to be addressed if e-voting schemes are to be used in untrustworthy environments. Firstly, methods to mitigate

threats posed by insiders are required; and secondly robust methods to authenticate the voter needs to be addressed. These issues need to be considered in any practical implementation of voting schemes if they are to be widely deployed.

6 Conclusion

Electronic voting systems are beginning to move from the lab to be deployed in the real world. Such systems have many potential benefits, however, at this stage there are some impediments that may leave the systems vulnerable in an untrustworthy environment.

In section 2 we presented a set of requirements that, if met, will overcome these impediments. We used these requirements to analyse two e-voting schemes that have recently been used in real elections and to consider how they would fare in an untrustworthy environment. Based on our analysis these schemes we saw the difficulty in preventing coercion resistance, vote buying and vote selling in the remote voting scheme – since a voter can be monitored whilst voting, or voted on behalf of. And with supervised voting schemes, we cannot always rely on traditional means and electoral officials to adequately authenticate voters.

We argue that in order to be deployed in less benign environments, e-voting schemes should be end-to-end verifiable right from authentication of voters to the tallying of votes. Fewer trust assumptions need to be made and less trust placed on voters, electoral officials and observers.

We appreciate that it is highly unlikely that voting schemes would completely eliminate human procedures and processes since security cannot be achieved by technology alone. However, we argue that where security could be provided by technological means, then this should be leveraged wherever possible in the electoral process.

We are currently investigating the use of smartcards and biometrics for authentication in supervised electronic voting schemes and the cost implications. We are also looking at end-to-end verifiable schemes using mix-networks to provide anonymity. We will also be investigating a means of providing individual verifiability whilst still satisfying receipt-freeness.

References

Abandah, G., Darabkh, K., Ammari, T., & Qunsul, O. (2014). Secure National Electronic Voting System. *Journal of Information Science and Engineering, Vol. 30 No. 4*, 1339-1364.

Anane, R., Freeland, R., & Theodoropoulos, G. (2007). E-Voting Requirements and Implementation. *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, (pp. 382-392).

Asunka, J., Brierley, S., Golden, M., Kramon, E., & Ofosu, G. (2013). *Protecting the polls: The effect of observers on election fraud*. Retrieved from http://cega.berkeley.edu/assets/miscellaneous_files/Asunka_etal_Protecting_the_Polls.pdf

Benaloh, J., & Tuinstra, D. (1994). Receipt-free secret-ballot elections. *In Proceedings of the twenty-sixth annual ACM symposium on Theory of computing (STOC '94)*, (pp. 554-553). Montreal, Quebec, Canada .

Burmester, M., & Magkos, E. (2003). Towards Secure and Practical E-Elections in the New Era. In D. A. Gritzalis, *Secure Electronic Voting* (pp. 63-76). Boston, MA: Springer US.

Burton, C., Culnane, C., & Schneider, S. (2015). *Secure and Verifiable Electronic Voting in Practice: the use of vVote in the Victorian State Election.* http://arxiv.org/abs/1504.07098.

Cabinet Office. (2009). *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.* London: Crown Copyright. Retrieved from http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

Chevallier-Mames, B., Fouque P, A., Pointcheval, D., Stern, J., & Traoré, J. (2010). On Some Incompatible Properties of Voting Schemes. In D. Chaum, *Towards Trustworthy Elections. Lecture Notes in Computer Science* (pp. 191-199). Berlin: Springer, Berlin, Heidelberg.

Clarkson, M. R., Chong, S., & Myers, A. C. (2008). Civitas: Toward a Secure Voting System. *2008 IEEE Symposium on Security and Privacy*, (pp. 354-368).

Cole, E. (2014, August). *Insider Threat in Law Enforcement. SANs White Paper*. SANs Institute. Retrieved from www.sans.org/reading-room/whitepapers/threats/insider-threats-law-enforcement-35402.

Craig, A. L., & Cornelius, W. A. (1995). Houses Divided: Parties and Political Reform in Mexico. In S. Mainwaring, & R. S. Timothy, *In Building Democratic Institutions: Party Systems in Latin America, eds* (pp. 249-297). California: Stanford: Stanford University Press.

Cramer, R., Franklin, M., Schoenmakers, B., & Yung, M. (1996). Multi-Authority Secret Ballot Elections with Linear Work. In U. Maurer, *Advances in Cryptology — EUROCRYPT '96: International Conference on the Theory and Application of Cryptographic Techniques Saragossa, Spain, May 12–16, 1996 Proceedings* (pp. 72-83). Berlin, Heidelberg: Springer Berlin Heidelberg.

Culnane, C., Ryan, P. Y., Steve, S., & Vanessa, T. (2015). vVote: A Verifiable Voting System. *ACM Transactions On Information and System Security*, 1-30.

Delaune, S., Kremer, S., & Ryan, M. D. (2006). Verifying Properties of Electronic Voting Protocols. *In Proceedings of IIAVoSS Workshop On Trustworthy Elections (WOTE'06)*, (pp. 45-52). Cambridge.

Dominguez, J. I., & James, A. M. (1998). *Mexicans React to Electoral Fraud and Political Corruption: An Assessment of Public Opinion and Voting Behavior*. Elsevier.

Feier, C., Neumann, S., & Volkamer, M. (2014). Coercion-Resistant Internet Voting in Practice. *44th Annual Meeting of the Society for computer science, computer science, Big Data - mastering complexity*, 1401-1414.

Ferree, K. E., Gibson, C. C., & Long, J. D. (2014). Voting behavior and electoral irregularities in Kenya's 2013 Election. *Journal of Eastern African Studies*, 153-172.

Fujioka, A., Okamoto, T., & Ohta, K. (1993). A practical secret voting scheme for large scale elections. In J. Seberry, & Y. Zheng, *Advances in Cryptology — AUSCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques Gold Coast, Queensland, Australia, December 13–16, 1992 Proceedings* (pp. 244-251). Berlin, Heidelberg: Springer Berlin Heidelberg.

Heiberg, S., & Willemson, J. (2014). Verifiable Internet voting in Estonia. *6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, (pp. 1-8).

Heskey, J., & Bowler, S. (2005). Local Context and Democratization in Mexico. *American Journal of Political Science*, 57-71.

Jan, J., Chen, Y., & Lin, Y. (2001). The design of protocol for e-voting on the Internet. *IEEE Annual International Carnahan Conference on Security Technology*, (pp. 180-189). doi:10.1109/.2001.962831

Jensen, P. S., & Justesen, M. K. (2014). Poverty and vote buying: Survey-based evidence from Africa. *An International Journal on Voting and Electoral Systems and Strategy*, 220-223.

Karr, J., & Wang, J. (1999). Towards a practical, secure, and very large scale online election. *Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual*, (pp. 161-169).

Langner, R. (2001). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy, 9*(3), 49-51. doi:10.1109/MSP.2011.67

Lehoucq, F. (2003). ELECTORAL FRAUD: Causes, Types, and Consequences. *Annual Review of Political Science*, 233-256.

Nichter, S. (2008). Vote Buying or Turnout Buying? Machine Politics and the Secret Ballot. *The American Political Science Review, vol. 102, no. 1*, 19-31. Retrieved from http://www.jstor.org/stable/27644495

Nichter, S. (2014). Conceptualizing Vote Buying. In H. D. Clarke, & G. Evans, *Electoral Studies An International Journal on Voting and Electoral Systems and Strategy* (pp. 315-327). Elsevier.

Schneier, B. (2009, 16 February). *Schneier on Security – Insiders*. Retrieved from Schneier on Security: https://www.schneier.com/blog/archives/2009/02/insiders.html

Schoenmakers, B. (1999). A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting. In M. Wiener, *Advances in Cryptology — CRYPTO' 99: 19th Annual International Cryptology Conference* (pp. 148-164). Santa Barbara, California: Springer Berlin Heidelberg.

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). Newyork.

Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J. (2012). Attacking the Washington, D.C. Internet Voting System. In A. D. Keromytis, *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Revised Selected Papers* (pp. 114-128). Berlin, Heidelberg: Springer Berlin Heidelberg.