Prova Scritta 09 Luglio 2020

Prova n. 1

Electronic voting

Context.

In the context of digital transformation, Regione Emilia-Romagna would like to test an electronic voting method for the next electoral round.
Electronic voting management methods may use different technologies, including:

- Voting by DRE (Direct Recording Electronic), e.g. Australia’s “Pret-a-Voter” scheme
- Internet Voting, the so-called 'i-Voting'

The DRE is a system that replicates the traditional voting infrastructure (booths at designated poll-sites) by integrating it with an automated system for collecting preferences.
The i-Voting method instead allows you to vote via the Internet.

Project goals.

The Region would like to simplify and digitize the voting operations for the election of regional council. The Region wants to reduce the organizational efforts related to the voting operations, while speeding up their management and reducing costs for the structures and resources involved. At the same time transparency, security, and traceability of voting operations must be guaranteed. It is therefore necessary to define the changes in the voting process and the characteristics of the supporting technology keeping in mind that three are areas need to be assured:

1) Identification of the voter
2) Impossibility of data manipulation
3) Freedom and secrecy of the vote

A review text is attached as a support reference.

Your task.

You are expected to propose an implementation of the projected goal, choosing one of the technologies to support it. The description should comply with the following item list:

1) Rappresentare sinteticamente il processo attuale e quello che viene proposto, evidenziando il ruolo delle tecnologie e motivando la soluzione scelta
2) Delineare l’architettura del sistema a supporto del nuovo processo, proponendo possibili tecnologie di sviluppo software, individuando le principali funzionalità applicative, uno schema ad alto livello dei dati coinvolti e i tipi di interfaccia utente richiesti

3) Definire il macro-piano di lavoro che identifichi le principali fasi e le reciproche relazioni di dipendenza, gli obiettivi di ogni fase, le competenze specialistiche necessarie
4) Individuare le modalità con le quali, garantendo la segretezza del dato sia possibile estrarre informazioni utili all’analisi del voto, descrivendo gli strumenti utilizzabili per la fruibilità dei dati per l’Ente e per i cittadini (logica OPEN DATA).

Allegato Prova Scritta n. 1

ANALYSIS OF ELECTRONIC VOTING SCHEMES IN THE REAL WORLD

(abridged version. Full text available at
https://pdfs.semanticscholar.org/26d4/7710ba37aa985dacf564e80562987abdd32f.pdf)

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.

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 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.

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. In Hong Kong, the largest and most sophisticated ever DDoS attack hit an online democracy poll that canvassed opinions for future elections in the country4. Also, in Ukraine a virus that was meant to delete votes during the presidential elections hit their Central Election Authority.

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 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.

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.

Threat	Vulnerability	Impact	Scheme
Poll-site officials vote on behalf of abstained voters.	Trust placed on poll-site officials to authenticate voters using traditional means as used in paper based elections. Ballots are not authenticated hence not digitally linked to voter.	Votes are cast for abstained voters without being detected by the system and could change the outcome of the election.	Pret-a-voter
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