Challenges in Designing an Electronic Voting System

Chris Dahlberg
Harvey Mudd College
340 E Foothill Blvd
cdahlberg@hmc.edu

Abstract

Since the disputed US 2000 presidential election, voting systems have come under increased public scruitany. Traditional systems have been criticized as too complicated and difficult to use. There has been a legislative push towards new electronic voting machines, generally incorporating touchscreen technology, that electronically record and tally each vote (DRE systems). These in turn have prompted public outcry about security problems. This paper lays out a set of criteria for a ideal voting system and examines the security issues of both traditional and DRE voting systems. Security in DRE systems is found to stem from trusting the DRE software while traditional systems depend on non-colluding poll workers.

1. Introduction

In recent years, electronic voting systems have largely replaced traditional hand-counted paper ballots in most states and counties. These new systems can be divided into two large categories: computer-counted systems and direct-read electronic(DRE) systems.

Computer-counted Marksense and punchcard systems still rely on a paper ballot. The voter either physically modifies the ballot or marks specific regions with a machine-readable carbon-based ink. Ballots are collected as normal and then tallies are computed using a computer to read the ballots. These are the most widely adopted form of voting system. Results are available at lower cost, more rapidly because ballots are no longer counted by hand. In recent years (following the contested 2000 presidential election), they have come under attack for being too confusing for voters and difficult to count.

DREs DRE systems are a more dramatic departure from traditional paper ballots. Instead of marking a printed sheet, voters are presented a computer monitor displaying the ballot choices. They make their selection using either a touchscreen interface or with simple buttons. The vote is recorded on the machine's internal storage and then transferred to a central repository for tabulation. There is generally no paper record and the machine's internal count is considered authoritative. DREs are generally sold as both lower cost and simpler to use than computer-counted paper systems. As their use spreads, concerns about the reliability and security of these devices are emerging. None of the existing commercial DRE systems adequately satisfies security demands. In this paper, the author examines the security demands on voting and how voting differs from other applications like commerce or secure communication where well-respected solutions exist.

The paper begins with a comparison of electronic voting with electronic banking transactions, an application generally considered secure. Next is a explanation of the properties of an ideal voting system. Each of the security-relevant properties is examined in turn and the advantages and disadvantages of DRE and traditional systems are discussed in each.

2. Comparison with Traditional Transactions

There are some arenas where electronic systems are highly trusted and reliable, well beyond the paper systems they replaced. Electronic bookkeeping and transaction management has entirely replaced manual record keeping. There is little outcry for increased security on financial transactions.

Information Segregation These systems differ from voting in that they are symmetric with regard to identifying the participants and information should never be lost. The merchant/bank can identify the client and the client can identify the bank throughout the transaction. In contrast, the preliminary stage of voting involves the polling station acquiring and verifying identifying information from the voter. On one level, this information must be retained to

prevent ballot-stuffing, but it can't be explicitly or implicitly attached to the vote itself. When a fraudulent transaction occurs, there is a complete record of all transactions that can be followed to determine the point of failure. No such record can legally exist for an election.

Cost of Failure Even in a banking system, errors and security failures do exist [2]. They occur at statistically predictable levels. Banks expect to lose some money to fraud and budget accordingly. User convenience and participation along with low levels of fraud is ultimately more economical than draconian security measures. This sort of loss is unacceptable in voting systems. Convenience for the majority isn't seen as a good excuse to disenfranchise a few.

3. Characteristics of the Voting Problem

Concerns in voting can be boiled down to a few simple concepts, described here. Valid elections must meet each of these concerns.

• **Privacy:** No other person should be able to tell how a voter voted. Even bulk statistics such as correlating vote with language should not be exposed. The only acceptable information disclosure is the final vote total for each precinct.

• **Lack of Evidence:** The voter should not be able to prove to anyone which way he has voted. Together with the privacy condition, this prevents vote-selling and coercion. If there is no way to assure a third party of which way a vote has been cast, bribes and threats are ineffective.

• **Fraud-Resistance:** Each qualified voter should be able to vote exactly once and no other persons should be able to vote. The system must verify the identity of each potential voter and determine their status, but must not allow this information to become associated with their vote.

• **Ease-of-Use:** Elections must serve the entire public. This includes people with various levels of technological familiarity, various languages, and various physical capabilities (vision, hearing, etc..). Any systemic bias in the error rates between these groups could unfairly alter the election results. Additionally, the poll workers running each voting stations have minimal training and technical skills. Setting up and administrating the system must be simple.

• **Scalable:** Large elections must serve millions of people. The system must scale to handle these elections as well as smaller precinct-specific ones.

• **Speed:** As a result of exposure to computer-counted ballots, the American public now demands that at least preliminary results are available within several hours of polls closing. Any voting system that requires lengthy counting time will not be acceptable.

• **Low Cost:** Cost is a major concern for counties selecting voting systems. A lower-cost, less-secure system is oftentimes more attractive than a higher-cost alternative. If a system can't be implemented cheaply, it isn't useful.

The ideal voting system should meet each of these criteria. In practice, no system is perfect and will sacrifice in one area for gains in another. Of these points, privacy, lack of evidence, and fraud resistance affect the security of the system. Ease-of-use affects the fairness of the system and scalability, speed, and cost affect the practicality. Generally, ease-of-use, scalability, speed, and cost are all in favor of DRE systems[4]. The properties of traditional (computer-counted paper ballots) and DREs in filling the security parameters will be examined in the remainder of this paper.

4. Privacy

Voting systems should not expose any information apart from vote totals. This is made difficult by the abundance of sidebands available to transmit information.

A sideband is a channel of communication internal or external to the system not explicitly designed to convey information. In poorly designed voting systems, sidebands can be used to determine how a person voted without breaking the security assumptions of the system.

4.1. Traditional Ballots

Ballot Design Traditional ballots generally provide weak privacy for atypical voters. Some voters can't use standard ballots. Some people want ballots written in their primary language. People with weak or no vision might need large-print, recorded, or Braille ballots. Elderly or infirm people may have difficulty with the fine motor skills needed to fill out marksense or punchcard ballots. In each of these cases, a special ballot will be needed. The voting preferences of each group can be determined because their ballots are physically different. Identifying information is conveyed accidentally through the design of the ballot.[3]

For example, consider a traditional paper ballot in a predominantly English-speaking precinct with a Spanish-speaking minority. The state is legally required to provide ballots and voting information in all major languages present in the precinct. If the Spanish-speaking citizens fill out Spanish ballots and the English-speaking citizens fill out English ones, poll workers sorting the ballots will be able to determine how each group voted. Even though no ballot is personally identified, private information has still leaked.

To prevent avoid this problem with traditional ballots, the state will need to provide a single ballot containing every necessary possibility. The ballots will quickly become complicated and expensive. In practice, the cost is prohibitive and less-private specialty ballots are used instead.[1]

Malicious poll workers Paper ballots also suffer from the possibility of malicious poll workers altering ballots to be

personally identifiable. A ballot can be marked fairly easily to pass a casual examination but still uniquely identify a voter.

For example, UV-sensitive ink could be used to mark each ballot. As voters generally don't examine their ballot under a blacklight before voting, this modification will almost assuredly go undetected. Later, the worker can examine the ballots and determine the vote. This problem can be mitigated somewhat by not allowing anyone who has physically handled the ballots before the election to view the completed ones, but this increases personal costs and is still insufficient if there is collusion[3].

4.2. DREs

DRE systems solve the problems of traditional ballots well. A single machine can store easily store many different versions of the ballot. Voters can select their preferred form in privacy. Once a vote has been recorded into memory, it is identical to every other vote and there is no way to connect it with a specific ballot form.

However, DREs are not a silver bullet against sideband communication. Depending on their implementation, they can expose additional sidebands. In the most extreme case, images on displays can be reconstructed from the emitted radiation, allowing outside parties to observe the vote. More realistically, timestamping information can be used in attacks. Many systems timestamp arriving votes. Without any other information, this is harmless and can actually improve security and service (for example, hundreds of votes within a few seconds is a sign of tampering, and flow information could help when planning polling station locations). However, suppose a malicious poll worker with access to the timestamps set up a camera in the polling station lobby. By combining a record of voter arrival times with the timestamp information, he could determine at how each person voted[1].

Even systems without explicit timestamp information can be exploited in this way. One common proposal in DREs is to print a summary of each voter's vote at the end of the transaction to allow the voter to verify that their choices have been entered correctly and provide a backup record to recount against (the record is physically separated from the voter by a clear partition so it can't be removed). The obvious way to implement this feature is using a spool of paper similar to that used in normal receipt-printing devices. However, the order on the spool effectively timestamps the votes.[2] Again, tracking the order people enter a voting station allows votes to be determined. Because they are built on top of general-purpose computers, this sort of information can be stored in unforeseen places. The Open-Vote system, for example, runs on top of a normal Unix filesystem and must go through additional steps to remove creation and access time from the files storing vote information[3]

5. Lack of Evidence

Both traditional and DRE systems do a good job of blocking peoples' ability to prove how they voted. Paper systems require voters to leave their completed ballot behind for the vote to count. DRE systems provide no evidence of votes apart from the internal storage and possibly a paper record, neither of which can be retrieved by the voter. Voters could get around this restriction by concealing recording devices and recording their vote from the privacy of the voting booth, but even this isn't absolute. A voter could record a marked ballot and then invalidate it and receive a new one. In both systems, there is no absolute evidence of a vote available, so coercion can be escaped and a briber can't guarantee that a bribee actually voted as instructed.

6. Fraud-Resistance

6.1. Duplicate Voters

Traditional and DRE systems usually use the same methods to prevent duplicate voters. The polling station verifies identification against a list of registered voters and then gives the voter a token allowing him to vote. In traditional systems, the token is generally the ballot itself. In DRE systems, the token can be a PIN, smartcard, etc... Coordinating between polling places to prevent duplicate votes at different stations is separate from the voting system itself.

6.2. Forged/Modified Votes

A second source of fraud is directly inserting forged votes or modifying existing votes. By inserting or removing a relatively small number of votes, the outcome of close races could be shifted.

Traditional In traditional systems, arbitrary individuals are prevented from forging votes by auditing and controlling who has physical access to blank ballot stock. The supply chain from the printer to the polling station is guarded. Once votes have been made, the excess ballots are destroyed and the completed ones are moved to the canvassing station in tamper-resistant containers and tallied. The system relies on trusting the workers who move the ballots and operate the counting machines. If sufficient workers collude, they could selectively invalidate ballots to produce a desired outcome. Security is created by requiring large numbers of poll workers to simultaneously collude.

DRE DRE systems are subject to different fraud and trust issues. Vote totals are cryptographically protected. After the polls close, the totals and information identifying the machine are encrypted with pre-programmed keys shared between the canvassing computer and the voting

machine[4]. To tamper with vote totals, an attacker must know the secret keys and the machine id. Since poll workers are not involved in key selection, there is less danger of workers altering counts. However, the system depends on trusting that the code running on each machine is correctly implemented and doesn't contain bugs or backdoors allowing unauthorized access. Modern commercial DRE systems are closed-source and can't be independently verified, so the public must trust the company producing the machine. Using a DRE shifts trust from the poll workers to the DRE company and the individuals involved with creating keys.

6.3. Auditing/Recounts

In any electoral system, allegations of voting irregularities are inevitable. When they do occur, it is desirable to have some backup count to validate the primary count against.

Traditional In traditional systems, close races are generally subject to hand recounts. Humans go back over the votes, manually counting each one. This allows poorly marked ballots that weren't correctly read by the machines to be counted. However, this introduces human subjectivity into the vote counting process. Some votes can reasonably be counted for multiple candidates or rejected completely. Subsequent recounts will rarely produce identical totals. Additionally, the process is length and expensive. It damages voter confidence in the validity of the election.

DREs DREs have the opposite problem. Instead of many interpretations for each ballot, there is only the electronically recorded count. Physical records of each vote are either not retained or not considered official. After an election there is little recourse except to accept the stated total at face value.

7. Conclusion

Overall, the security difference between DREs and traditional voting systems is where trust is placed. Traditional systems are based on the belief that large numbers of poll workers don't collude. Sufficiently large numbers of malicious workers can easily manufacture new votes, identify other people's votes, or destroy legitimate votes. Security measures are aimed around raising the required number of colluders.

DRE systems require trusting fewer people, but those people have much larger responsibilities. Only error or maliciousness by the designers and those who set keys can result in the destruction or exposure of votes. However, designing a correct and secure system in any field is notoriously difficult and there isn't a long history of developing DREs to flush out problems. The computer systems running DREs are more complicated than traditional systems and more difficult to design. Since identical software and hardware is distributed throughout a precinct, a single error in a DRE system can have a much larger effect on an election than in a traditional system.

The decision on whether to implement a DRE or use a traditional method is largely based on competing tradeoffs. DREs are cheaper than traditional systems and capture voter intent more effectively, but are more subject to fraud problems. None of the problems with DREs are inherent to the design or unsurmountable, but will require time and experience to work out. Adopting DREs will likely involve accepting decreased security while issues are solved.

References

[1] B. Bederson, B. Lee, R. Sherman, P. Hernson, and R. Niemi. Electronic voting system usability issues. *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 145–152, 2003. 2, 3

[2] A. Keller, A. Dechert, K. Auerbach, D. Mertz, A. Pearl, and J. Hall. A pc-based open-source voting machine with an accessible voter-verifiable paper ballot. *Open Voting Consortium*, 2004. 2, 3

[3] A. Keller, D. Mertz, J. Hall, and A. Urken. Privacy issues in an electronic voting machine (short abstract, full article linked). *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 33–34, 2004. 2, 3

[4] A. Xenakis and A. Macintosh. E-voting: E-electoral administration: organizational lessons learned from the deployment of e-voting in the uk. *Proceedings of the 2005 national conference on Digital government research*, pages 191–197, 2005. 2, 4