

# **Online Voting: A Replacement for Physical Ballots?**

Sam Bradley  
Composition 3130

for  
Dr. Jo Mackiewicz  
Technical Writing Instructor  
University of Minnesota-Duluth  
Duluth, Minnesota

*November 24, 2004*

## Abstract

Currently the U.S. uses a physical-ballot system in presidential elections. This system has been sufficient thus far, but has been criticized recently. The system is criticized because it is inconvenient of the system, inaccurate, and the likely to be exploited through attempts of fraud. An alternative to this physical-ballot system could be the use of an online-voting system. The aim of this report is to determine the feasibility of such a system. It was found that an online-voting system would be feasible for use in a presidential election in the U.S. within the next two elections (2012).

## Introduction

**Purpose:** This report determines the feasibility of an online-voting system to be used in place of physical ballots for a presidential election in the United States.

**Problem:** The current ballot system used for elections the United States can create problems. One of these problems is a declining voter turnout [1]. A common reason for this decline is the inconvenience of having to go to the polls, but also, many people are unable to go to the polls. These people might be out of town, or simply too busy to make it to the polls [2]. Another problem is that the current ballot system can be extremely confusing. In the 2000 presidential election, Palm Beach County in Florida used a butterfly ballot that is known for the amount of confusion it caused [3]. The ballot was unclear as to which mark corresponded to which candidate (see Figure 1 below).



Figure 1: Confusing butterfly ballot

**Scope:** This report investigates the feasibility of using an online-voting system and whether or not it is feasible to use such a system in a presidential election in the United States by the year 2012. These considerations include (1) security of the system, (2) simplicity and accessibility of the system, and (3) accuracy of the system.

## Discussion

### *Criterion 1: Security of the System*

**Explanation.** The security of an online-voting system is a large concern. There are two areas of concern relating to security issues: fraud and voter privacy. The current ballot system allows the possibility of fraud, but it is generally tolerated because the system is localized, making it unlikely that a successful fraud would extend beyond a single district [4]. An online-voting system could be accessed anywhere, which could be a potential danger. Voter privacy is not a problem using the current system, but would be an issue using an online system. Unwanted parties could potentially intercept voter's information during transmission.

**Data.** Some security methods have already been tested and implemented. The Arizona Democratic Party held the first online election in March of 2000 in its presidential preference primary [5]. The election was held by *election.com*. To ensure fraudulent activity did not take place during the election, an accounting firm, KPMG, was hired to monitor the system's security. The firm generated two encryption keys, a public key and a private key. The public key was available to people to enable them to encrypt their vote. The private key was not available to anyone but the private firm so that only they would be able to decrypt the ballots. At the same time, the private firm did not have access to the encrypted ballot until after the election [5]. This process is modeled in Figure 2 below.

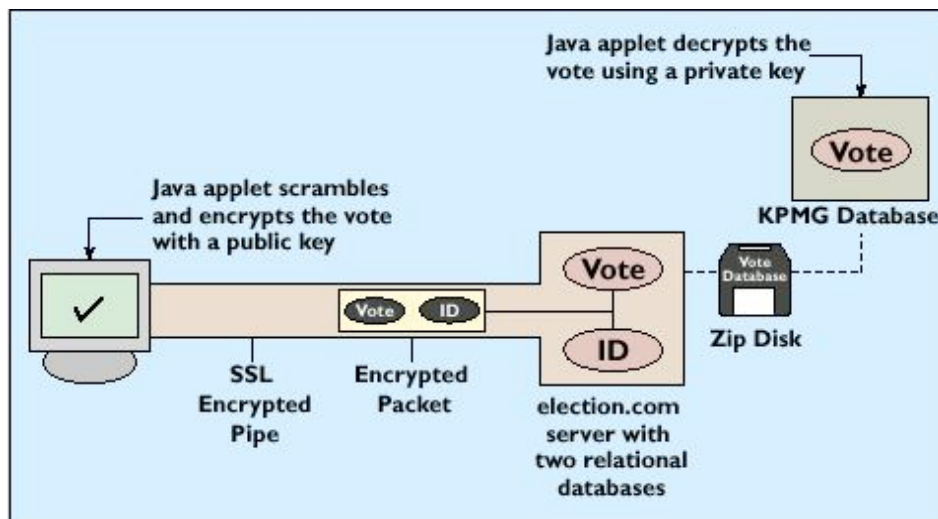


Figure 2: Encryption and Decryption of Votes. A java applet running on the voter's computer encrypts the vote so that no one can read it. It is then stored in a database until the election is over. The private firm holding the key to decrypt the packet doesn't have access until this time.

To ensure voter privacy, a voter's identification was kept in a separate relation from the vote.

Another method to ensure voter privacy is to use a blind signature. In order to verify if a registered voter is sending a ballot, the system needs to know whom the voter is. A digital signature can be used to determine who sent the message. A blind signature allows a person to sign a message without revealing the content of it [6].

**Interpretation.** These methods offer a reasonable amount of security within the system. Problems may arise due to the third-party firm that decrypts the votes. It would potentially be possible for the firm to alter votes during decryption. Because it is unknown how the votes are decrypted, it would be possible for the firm to claim votes were decrypted in such a way and yet actually decrypt in another. This problem would need to be considered before using an online-voting system for a nation-wide election.

## *Criterion 2: Simplicity and Accessibility of the System*

**Explanation.** In order for an online-voting system to be successful, it needs to be something anyone can use [2]. This condition requires (1) the system must be simple enough that anyone can understand it and (2) the system must be accessible to anyone. If the system were made too complicated, it wouldn't add any benefit from the current ballot system. The risk that voters would not understand how they were placing a vote would be the same if not greater than that of the current ballot system. Similarly, the voter turnout would not benefit if the system weren't accessible to everyone. The idea behind an online-voting system is that it would be more convenient for people, but a system that isn't accessible doesn't add any convenience. Not only would a system that wasn't accessible not appeal to people who wouldn't use the current ballot system, but also it would discourage people that otherwise would have voted.

**Data.** The Democratic Party of Arizona used multiple methods to ensure that all registered voters were able to cast their vote. To educate voters on how to use the system, the party advertised a tutorial in a number of ways including print publications and both radio and televised broadcasts [5]. For voters that were unable to use the system, physical voting locations were still offered where a person could cast a paper ballot. These physical locations also offered voters that didn't have Internet access to vote. Voters were able to vote either by paper ballot or by Internet using a supplied computer [5].

**Interpretation.** In the 2000 primary, the Democratic Party of Arizona made sure all registered voters were able to vote. Even if the system wasn't simple enough or available to a person, a voter was still able to cast a vote at a physical location. The problem in using physical locations is that they defeat some of the main purposes for holding an online election; it would cost less to not use these locations and the results can be determined much faster.

### *Criterion 3: Accuracy of the System*

**Explanation.** As with any method, an online-voting system must take an accurate tally. An online system opens opportunities for a number of mistakes to take place while counting ballots. The system must ensure these precautions to be accurate: (1) a vote cannot be altered or duplicated, (2) only a registered voter can vote, (3) a voter can place only one vote, and (4) only the voters can place their own vote.

**Data.** To ensure these things, *election.com* used two database relationships in the 2000 Arizona presidential preference primary. The first relation kept a tally of the votes. The second relation held information about voters. This information included the voter's registration information and whether or not they had already cast a vote. If the database determined that the voter was registered and had not already voted, it would add the vote to the relationship containing the tally excluding any information about the voter. The database would then change the relation containing the voter's information to indicate that he or she had already voted [5]. Figure 3 below illustrates this relation.

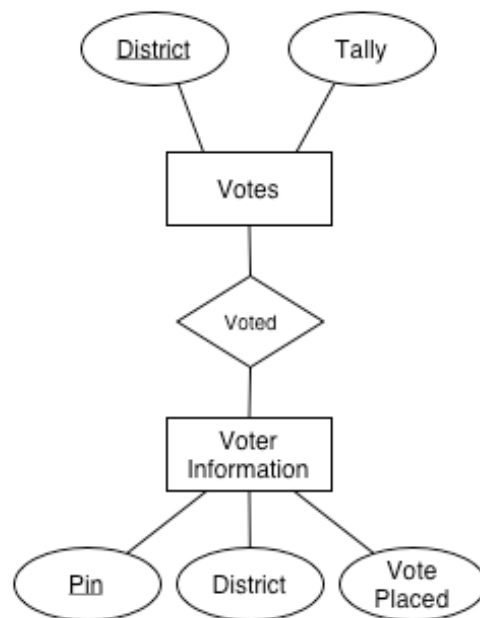


Figure 3: Database relationship. The database consists of two tables: the voter information and the votes. Voters are able to place a vote in the votes table, but no information about the voter is stored in the votes table.

To ensure that only voters could place their own vote, *election.com* sent out personal identification numbers to registered voters. These numbers were used to authenticate the voter. If a voter requested a mail-in ballot, their pin would be void, ensuring that they would not be able to vote twice [5].

**Interpretation.** This relationship model ensures all the things necessary to be accurate. Registered voters are authenticated and allowed only one vote. Using the personal identification number, the system can be certain that the vote is being sent by the person the voter claims to be. Because this number contains seven digits, there are two billion possible pins. This amount makes it difficult to associate an identification number with an individual person [5]. The model also adds to the security of voter privacy because information about the voter is kept separate from how he or she voted.

## Conclusion

**Summary.** To be successful, an online-voting system only needs to compare to the current physical system [6]. Using some of the methods discussed in this paper, a system could be created that would come close. There are still some issues that need to be worked out. Currently, a nation-wide election using an online system would not be a good idea due in part to skepticism of such a system's success. Within the next two elections, with some changes, an online-voting system may be a possibility, but an online-only election would take longer.

**Contact Information.** Please direct questions to: Sam Bradley at [brad0250@d.umn.edu](mailto:brad0250@d.umn.edu)

## References

- [1] A.-M. Oostveen, "E-voting and the democratic process: E-voting around the world" [presentation] *e-Ping meeting Brussels*, September 10<sup>th</sup>, 2002.
- [2] J. Karro, J. Wang, "Towards a Practical, Secure, and Very Large Scale Online Election" *Computer Security Applications Conference*, pp. 161-169, 1999.
- [3] R. Mercuri, "Better Ballot Box?" *Spectrum*, vol 39.10, pp. 46-50, 2002.
- [4] A. D. Rubin, "Security Considerations for Remote Electronic Voting" *Communications of the ACM*, pp. 39-44, 2002
- [5] J. Mohen, J. Glidden, "The Case for Internet Voting" *Communication of the ACM*, vol 44.1, pp. 72-85, 2001.
- [6] S. Ibrahim, M. Kamat, M. Salleh, and S.R.A.Aziz, "Secure E-Voting with Blind Singnature" *Telecommunication Technology*, pp.193-197, 2003.