Analysis of the Security of Proposed Internet Voting Systems

Victor S. Andrei  
George Mason University  
vandrei@gmu.edu

Srinidhi Sreepad  
George Mason University  
ssreepad@gmu.edu

The introduction of Internet voting in the United States and other countries may potentially improve participation in elections by the young, the disabled, rural voters, citizens living and working overseas, and the military [1]. However, the development of Internet voting technologies has been marked by controversy in the United States, including the successful penetration of the 2010 Washington, D.C. Internet voting pilot by researchers at the University of Michigan [7], as well as the failures of Operation BRAVO and Project SERVE in the United States in 2004 [1]. Subsequently, the security of Internet voting systems has drawn scrutiny from the public at large and is even the subject of an ongoing massively open online course offered by Coursera [6].

The safety and soundness of elections is fundamental to the maintenance of democratic self-governance in nations such as the United States. With the growing movement towards the leveraging of the Internet and computer technologies to conduct elections, the issue at hand is whether Internet voting technologies can support “safe and sound” elections.

Relevant Work

We have identified a number of relevant sources, such as [1], which provides a history of voting systems in the United States, leading up to the introduction of Internet voting. [4] and [5] give an overview of Internet voting in other countries, including an analysis of the results of Swiss Internet voting pilots over the past ten years. The massively open online course on the history of election security in the United States is at [6], while [2] contains the cryptographic background needed to evaluate different Internet voting schemes with respect to the requirements for what constitutes a “secure” election. [2] also suggests a taxonomy for categorizing voting schemes.

Additionally, Grimm [8] and Neumann [9] define a set of requirements for electronic voting systems, including Internet voting systems. [10] and [11] illustrate a method for evaluating such systems. Lastly, we identified proposed Internet voting technologies that we plan to investigate, including VoteBox [12], Helios [13], Sensus [14], and others [15-23].

Plan of Investigation

We intend to examine a number of proposed Internet voting technologies with regard to their abilities to ensure that a given election is “safe and sound.” In our investigation, we will define a set of baseline requirements that must be met in order to conclude that a given election is “safe and sound.” Such a standard would include the following requirements:
- Only eligible voters may vote in a given election (voter eligibility and authentication);
- Each eligible voter may vote only once in a given election and may not vote on behalf of any other eligible voter (one man-one vote);
- Only individual voters should know the contents of their ballots (ballot secrecy);
- Individual voters should be able to verify the accuracy of their ballots (ballot verifiability)\(^1\);
- Individual voters should not be able to prove to a third party the contents of their ballots (resistance against election buying, chain voting, and other attacks);
- Each ballot should not be subject to tampering and should match the intent of the voter who cast the ballot (ballot integrity);
- All eligible voters should have the opportunity to vote (voter enfranchisement);
- The system should provide tools for auditing the results of a given election as well as the operations of the system’s software and hardware (audit capability);
- The system should provide a paper-based backup (paper-based backup);
- The system should be easy to use by individual voters, including individual voters with disabilities (usability); and
- The system should be available during the course of a given election (availability).

Additionally, Internet voting systems should be resistant to malware, including Trojan horses, viruses, and worms, and third-party hacking attempts that may change the outcome of the election.

We plan to develop a means of classifying different Internet voting systems based on the degree to which each system satisfies our standard. Thus, we will be able to conclude that the proposed Internet voting system that best meets our standard is the one most likely to ensure a “safe and sound” electoral outcome. Lastly, we plan to examine the role of Internet voting technologies in the overall election processes of nations such as the United States.

**Questions to Answer**

We will answer several questions as part of our investigation, including the following:

1. What Internet voting systems have been proposed in the past ten years?
2. What are the defining characteristics of an Internet voting system that ensures a “safe and sound” electoral outcome?
3. How can Internet voting systems be effectively classified?
4. How can the security of each particular proposed Internet voting system be improved to better ensure that an election held with such a system is “safe and sound”?
5. What advantages, if any, could be obtained from combining Internet voting systems with existing voting systems (e.g., Direct Recording Electronic and optical mark-sense)? How do Internet voting systems fit in to the overall election process?

\(^1\) [24] and [25] examine verifiability. As part of this project, we intend to think about how an Internet voting system could potentially provide ballot verifiability to individual voters.
Verification Procedures

Aside from implementing and testing the different Internet voting systems in actual, live elections, or through a pilot election, there are no effective ways to compare the “real world” ability of the proposed Internet voting systems against existing voting systems such as Direct Recording Electronic or optical mark-sense ballots. We could, however, design and implement a model Internet voting system that fully meets our requirements and builds upon existing proposals. We could test this implementation in a pilot election in our class, time permitting.

Timeline

We intend to conduct our research based on the following timeline, which is approximate and subject to change based on the progress of our project.

<table>
<thead>
<tr>
<th>Week</th>
<th>Activities</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct. 8-14</td>
<td>• Determine requirements for what constitutes a “safe and sound” election.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Review the proposed Internet voting systems. Discard any systems that are</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Analyze. Add new systems that we discover.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Question 2]</td>
<td></td>
</tr>
<tr>
<td>Oct. 15-21</td>
<td>• Finish activities from previous week. [Question 1]</td>
<td>Progress Report 1</td>
</tr>
<tr>
<td>Oct. 22-28</td>
<td>• Develop a system for classifying proposed Internet voting schemes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Question 3]</td>
<td></td>
</tr>
<tr>
<td>Oct. 29-Nov. 4</td>
<td>• Classify the Internet voting systems that we have identified.</td>
<td>Progress Report 2</td>
</tr>
<tr>
<td>Nov. 5-11</td>
<td>• Develop improvements to each Internet voting system that we have identified.</td>
<td>[Question 4]</td>
</tr>
<tr>
<td>Nov. 12-18</td>
<td>• Finish activities from previous week. [Question 4]</td>
<td>Progress Report 3</td>
</tr>
<tr>
<td>Nov. 19-25</td>
<td>• Analyze where Internet voting fits into the overall election process.</td>
<td></td>
</tr>
<tr>
<td>Nov. 26-Dec. 2</td>
<td>• Finish activities from previous week. [Question 5]</td>
<td>Progress Report 4</td>
</tr>
</tbody>
</table>

Areas for Potential Change

During the course of our investigation, we may identify additional proposals for Internet voting systems and discard existing proposals that we deem are too simple or otherwise not appropriate for this project. We may discover that no existing proposal fully meets our standard for what constitutes a model Internet voting system that ensures that an election is “safe and sound.” Furthermore, we may discover that no existing proposal fully meets a given requirement within our standard. We may seek to develop our own model system that satisfies our requirements.
Tentative Table of Contents for Final Report

1. Introduction
2. What makes an election “safe and sound”?
3. Analysis of proposed Internet voting systems
   a. Sensus
   b. VoteBox
   c. Helios
   d. Other systems
4. Results; discussion
5. Improvements to proposed Internet voting systems
6. Our “model” Internet voting system
7. The role of Internet voting within the election process

References


