Requirements for an Electronic Voting System

Prashanth P. Bungale and Swaroop Sridhar
Department of Computer Science
The Johns Hopkins University

(i) Functional Requirements

1. Mobility: The voter should not be restricted to cast his ballot at a single poll-site at his home precinct.

- *Realistic*: He shall be able to vote from any poll-site within the nation.
- *Unrealistic/Expensive*: He shall be able to vote from any county-controlled kiosk (situated at public places such as banks, shopping malls, etc.) within the nation. (*Unrealistic* because of logistical and cost issues).
- *Infeasible*: He shall be able to vote from virtually anywhere using an Internet connection. (*Infeasible* both for technical security issues as well as social science issues).

2. Convenience: The system shall allow the voters to cast their votes quickly, in one session, and should not require many special skills or intimidate the voter (to ensure *Equality of Access to Voters*).

3. User-Interface: The system shall provide an *easy-to-use* user-interface. Also, it shall not disadvantage any candidate while displaying the choices (e.g., by requiring the user to scroll down to see the last few choices).

4. Transparency: Voters should be able to possess a general knowledge and understanding of the voting process.

5. Flexibility: The system shall be flexible in that it allows a variety of ballot question formats including open-ended questions (e.g. Write-in candidates and survey questions).

6. Support for Disabled Voters: The system shall cater to the needs of physically challenged voters (e.g. blind voters).

7. Accuracy: The system shall record and count all the votes and shall do so correctly.

8. Eligibility: Only authorized voters, who are registered, should be able to vote.

9. Uniqueness: No voter should be able to vote more than once.

10. Auditability: It should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records, in terms of physical, permanent audit trail (which should not reveal the user's identity in any manner).

11. Voter Confirmation: The voter shall be able to confirm clearly how his vote is being cast, and shall be given a chance to modify his vote before he commits it.

12. To issue Receipt or not?

- The system may issue a receipt to the voter *if and only if it can be ensured that vote-coercion and vote-selling are prevented*, so that he may verify his vote at any time and also contend, if necessary.

13. No Over-voting: The voter shall be prevented from choosing more than one candidate / answer.

14. Under-voting: The voter may receive a warning of not voting, but the system must not prevent undervoting.

15. Provisional Ballots: The voter shall be able to vote with a provisional (electronic) ballot if he has some registration problems, which could be counted if verified by the authorities later.

16. Documentation and Assurance: The design, implementation, and testing procedures must be well documented so that the voter-confidence in the election process is ensured.

17. Cost-effectiveness: Election systems should be affordable and efficient.

(ii) Security Requirements

1. Voter Authenticity: Ensure that the voter must identify himself (with respect to the registration database) to be entitled to vote. If voting other than at his home precinct, the voter may be asked to show some legal identification document.

2. Registration: The voter registration shall be done *in person* only. However, the computerized registration database shall be made available to polling-booths all around the nation.

3. Voter Anonymity: Ensure that votes must not be associated with voter identity.

4. System Integrity: Ensure that the system cannot be re-configured during operation.

5. Data Integrity: Ensure that each vote is recorded as intended and cannot be tampered with in any manner, once recorded (i.e., votes should not be modified, forged or deleted without detection).

6. Secrecy / Privacy: No one should be able to determine how any individual voted.

7. Non-coercibility and No Vote-selling: Voters should not be able to prove to others how they voted (which would facilitate vote selling or coercion).

8. Reliability: Election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of network communication. The system shall be developed in a manner that ensures there is no malicious code or bugs.

9. Availability: Ensure that system is protected against accidental and malicious denial of service attacks. Also, setup *redundant communication paths* so that availability is ensured.

10. System Disclosability: The core of the system, especially the vote-casting equipment, shall be *open-source*, so that it can allow external inspection and auditing.

11. Simplicity: The system shall be designed to be extremely simple, as complexity is the enemy of security.

12. Testing and Certification: The system should be tested by experts with respect to all of the security considerations, so that election officials have the confidence that the system meets the necessary criteria.

13. System Accountability: Ensure that system operations are logged and audited.

14. Personnel Integrity: Those developing and operating the voting system should have unquestionable records of behavior.

15. Operator Authentication and Control: Ensure that those operating and administering the system are authenticated and have strictly controlled functional access on the system.

16. Distribution of Authority: The administrative authority shall not rest with a single entity. The authority shall be distributed among multiple administrators, who are known not to collude among themselves (e.g., different political parties).