A Secure e-Voting System

Project Requirements

CS 600.443 Security and Privacy
Spring 2003

Team: Jamie Brown
Domari Dickinson
Carl Steinebach
Jeffrey Zhang

Secure e-voting System

Requirements Document

1 System Objectives

1.1 This e-voting system provides a voting service that allows people to vote from any poll site in the country electronically. This system encompasses legal, regulatory, behavioral, and sociological aspects of the current voting system, while adding additional convenience and security to the overall voting process.

1.2 This system is designed to improve the current voting process in the following ways:

- 1.2.1 Allow voters to vote from any poll site in the country without the use of absentee ballots *
- 1.2.2 Reduce the number of legitimate votes not counted by reducing the number of over-votes, and eliminating vote tampering
- 1.2.3 Improve the registration process by allowing voters to check their registration status prior to voting and centralizing registration databases
- 1.2.4 Increase voter confidence and improve the voting experience

2 Functional Requirements

2.1 Voter Registration

- 2.1.1 It must be easy for an individual to register to vote
- 2.1.2 An individual must identify themselves, in some way, in order to register
- 2.1.3 Prior to voting a voter may check his registration status*
- 2.1.4 A voter may register to vote on the day of the election*

2.2 Casting a Ballot

- 2.2.1 The voter must identify themselves, in some way, in order to vote
- 2.2.2 The process of casting a ballot should accommodate disabled and multilingual voters *
- 2.2.3 All possible choices must be displayed on a single screen
- 2.2.4 Record the selection of individual vote choices for each contest
- 2.2.5 Indicate that a selection has been made or canceled
- 2.2.6 Notify the voter when the selection is completed
- 2.2.7 Before the ballot is cast, the voter is allowed to review his choices and, if he desires, to delete or change his choices before the ballot is cast
- 2.2.8 Prevent the voter from over-voting
- 2.2.9 Notify the voter after the vote has been stored successfully that the ballot has been cast
- 2.2.10 Incorporate a visual indication of system status

2.3 Tallying the Ballots

- 2.3.1 An unofficial in-precinct vote tally will occur once the polls have officially closed

2.3.2 Votes will also be transferred to a central location to be officially tallied

2.4 Certifying the Vote
- 2.4.1 The number of votes cast should be consistent with number of voters
- 2.4.2 If a discrepancy exists, the audit trail should provide information regarding a voter's intent *
- 2.4.3 Recounts must be possible

3 Security Requirements

The security requirements for this system span all aspects of the voting process and include voter authenticity, voter anonymity, data confidentiality, data integrity, system accountability, system integrity, system availability, system assurance, and system reliability

- 3.1 An individual not registered to vote must not be able to cast a ballot
  - 3.1.1 A voter must not be able to vote more than once
- 3.2 The privacy of the vote has to be guaranteed during the casting, transfer, reception, collection, and tabulation of votes *
- 3.3 No voter should be able to prove that they voted in a certain way
  - 3.3.1 None of the participants involved in the voting process (organizers, election officials, trusted third parties, voters, etc) should be able to link a vote to an identifiable voter
- 3.4 Each vote is recorded precisely as the voter intended
  - 3.4.1 Each voter is ensured a "clean slate" of the system to ensure equality, confidence, and minimize system tampering
  - 3.4.2 The outcome of the voting process must correspond to the votes cast
  - 3.4.3 It should be infeasible to exclude a valid vote from the tabulation, and to validate a non-valid one
- 3.5 System and voter operations are logged and audited
- 3.6 The system cannot be re-configured during operation*
- 3.7 Access to voted ballots is prohibited until after the close of the polls
- 3.8 Additional ballots cannot be cast once the polling place has closed
- 3.9 The system must be open to independent inspection and auditing
- 3.10 The system is protected against accidental and malicious denial of service attacks *

* This group feels that these requirements are out of the scope of this project