Rashidat Agbaje
JaTara Brown
600.443
February 20, 2003

Project Requirements

Overall Requirements:

The basic requirements are two-fold: The system must be as secure as possible, yet be user-friendly and trusted by the public.

Functional:

1) The system must be cost-efficient (this is required by the project guidelines).
2) It should be user friendly; voters should not feel inconvenienced.
3) It should be redundant in that each ballot must be transmitted to the voter's home county at specified intervals, yet a copy remains at the local county server where the voter cast his vote as a backup.
4) The voter's identifying information should be stripped before the ballot is tallied.
5) The system must be in compliance with Federal Voting Rights Act.
6) The system must be auditable in form of a voter-verified paper trail or similar mechanism, i.e. a FROG in case of recounts.
7) The system should handle different formats, not just electronic, i.e. Braille ballots for the blind, multi-language written/electronic formats for ESL persons, etc.
8) The system should be optional, with current voting system as an alternative
9) Confirmation of vote cast is required, maybe in the form of a printout or FROG or a simple on-screen message saying "Your vote has been recorded."
10) Any paper methods should eliminate ambiguity of any kind (no dangling/dimpled/pregnant chads, no tentative marks on optical scanning sheets).
11) Each vote should be counted independently, i.e. voters are able to abstain from voting for a particular office without invalidating the entire ballot – although in this case, the system should warn them that their vote for a particular office has not yet been selected.

Analysis of Functional Requirements:

Requirements #1, 7, and 10 might be too expensive or unrealistic while the other requirements we believe we can meet.

Security:

1) There needs to be a methodology of securely calling up ballots appropriate for a particular voter, should the voter decide to vote outside of his home county.
2) When the ballot is transmitted to user's home county (if user voted away from home), the ballot itself must be encrypted as well as the communication between both counties.

3) Once a ballot has been cast, no one should be able to modify or delete it in any way without being detected.
4) There should only be one ballot per voter, regardless of where the voting takes place.
5) The system must be thoroughly tested for possible bugs.
6) The system must have back-up methodology of casting votes should the system go down (perhaps in the form of paper ballots).
7) Voters should be able to verify their ballot choices before actually casting their vote.
8) When the vote is cast and transmitted, identifying information and actual ballots should be sent on different channels, never simultaneously (this assumes that record keeping on each registered voter is maintained by local counties).
9) There should be a secure and speedy method of "checking off" voters so one person can't vote in one county, drive to another county, and place another vote in that county.
10) The system must log detailed anomalies with each machine for auditing purposes.
11) If a non-remote electronic poll site voting (no at-home Internet voting) option is selected, the poll site itself must be secure and sanctity of vote preserved (no electioneering, etc).
12) The system must use some form of redundancy in order to avoid having a single point of failure (maybe each county carries the total tally of at least 2 other counties).
13) The system must use the strongest and most appropriate cryptographic protocols during ballot retrieval, encryption, and transmission.
14) In auditable systems, the voter-verified media (printouts, FROG, etc) must be placed in a secure area, i.e. locked box and stored in a secure location until a recount/audit is needed.
15) The counting system should be accurate and verifiable by independent means (paper trail, etc).
16) The voter registration system must be trustable, i.e. there needs to a methodology for keeping the database updated and purged of non-eligible voters due to address changes or deaths. There also needs to be a way for the voter database to be shared among counties for voter authentication on Election Day.

Analysis of Security Requirements:

Requirements #5, 10, and 11 might be too expensive or unrealistic while the other requirements we believe we can meet.