CALTECH/MIT
VOTING TECHNOLOGY PROJECT

A multi-disciplinary, collaborative project of
the California Institute of Technology – Pasadena, California 91125 and
the Massachusetts Institute of Technology – Cambridge, Massachusetts 02139

CERTIFICATION AND VOTING SOFTWARE: POSITION STATEMENT

Ted Selker
MIT

Key words: ***voting software, electronic registration software, electronic voting machines, backend tally counting systems, software certification***

VTP WORKING PAPER #15
April 2004

National Academies

Committee on Building Certifiably Dependable Systems
Workshop on Certifiably Dependable Software
Georgetown University Conference Center
April 19-20, 2004

Certification of Voting Software; Position Statement

Ted Selker selker@media.mit.edu
Caltech/MIT Voting Project

Overview

Computers are important in every aspect of modern life. Automatic tabulating machines are designed to be the most consistent and reliable counting approach invented. Still, questions of reliability, security and auditablity persist. Ken Thompson and others have shown that, like other carelessly composed processes, computer programs can harbor potentially criminal activity. To be useful for voting, software must simplify and improve the ability to record and report intentions.

Best practices must be used in creating important software to guard against bugs and malware. In spite of the fact that malware can be hidden in any program, there are ways to assure that it is not impacting the operation of the software. First, test vectors must allow testing of the software in every conceivable situation. Second, demonstrations can be arranged to show that it is running correctly when it is actually used. Third, computers can produce multiple records to assure that it has performed correctly.

Electronic Registration Software.

Registration databases are thought to be the greatest loss of votes in the system. Registration databases are cleaned, updated and deployed with inadequate controls. Improvements to certifying this process could save 1 to 2 % of US votes.

Electronic Voting Machines

Electronic voting machines are used in many parts of the world to collect votes. They can be used to protect the ballot box from many kinds of stuffing, stealing and vandalism. They can be used to give voting independence to people with physical, perceptual, and cognitive special needs. They can simplify voting with multiple languages or illiteracy.

Improvements to certifying this software must also improve ballots which could save least 1% of US votes.

Backend Tally Counting Systems

The tally and election certification process has embraced software for years. Even with software, many cases of one person changing the tallies have been reported.

Certification Goals

Many opportunities are available to make and certify software to increase the ability for election results to reflect voter intentions. Computer experts' part of the certification process has to have teeth but not increase probabilities of problems. Open systems can allow public vetting; it also allows criminals to study and plot against potential weaknesses. Qualification processes for writers of crucial software are possible. Legacy systems cobbled together over years are potentially are thoroughly tested yet full of bugs. Finally, systems can be built and tested that give internal oversight of software. We have created demonstration N-Version software to avoid any single point of failure.

While code reads can find problems, in the end, good software is theoretically problematic and testing is crucial. Test vectors in voting will include and require more than a program that runs through the steps of the process. Testing voting software will require defense-in-depth approaches. All voting software components must be shown to improve acquisition, retention, and reporting of voter intention over systems it replaces. This means that the software and processes around it must be vetted. Today's computers allow adjustment of their time clocks. While a potential source of problems itself, this can be used to test for fraud. Setting the time to the beginning of an election, the actual situation of an election can be simulated to demonstrate built-in software fraud. Parallel testing can be done on the day of elections in which phantom precincts are voted, carefully demonstrating any systematic software reason that the election shouldn't be certified.

The clear separation and dependence on computer tasks has been made obvious in voting. Internal or external verification of the correctness of voting software actions seems important. External verification of software's correct handling of votes can be accomplished by video or audio transcripts, which do not add complex cognitive tasks for voters. End-to-end demonstration of vote deposit for voters is another goal. Voting software certification will be process in which testing and practices will continue to develop, hopefully to be useful for improvement of all human-computer systems.