Electronic Voting System Best Practices

Friday, March 11, 2005

Abstract: A brief best practices recommendation for robust trustable electronic voting systems that can not only detect errors but correct errors, written by, with revisions by, citizen coalition groups and computer scientists specializing in voting and elections systems who are dedicated to honest accurate elections. We urge that electronic voting systems produce a paper ballot that will enable the voter to verify that his votes are correct before casting those votes. This voter verified permanent record will permit a check on machine accuracy and make a truly auditable recount possible. Notably, it is not the mere presence of paper that secures the system: is the intrinsic independence of the paper and electronic records and the fact that both were witnessed by the voter that makes the system auditable. The attached document offers recommendations to aid in the design of requirements for voting equipment and election-technology legislation. The suggestions err on the side of safety.

Basic principles for trustable elections

1) It is not enough that elections be accurate, they have to be provably so and in a manner transparent to voters.

2) Errors will occur. We must design systems that can catch and recover from errors, rather than try to design systems that require unachievable levels of perfection in hardware, software, and operators.

3) Innocent anomalies will occur. Without open systems, errors, fraud, and innocent anomalies appear indistinguishable; for elections to be trustable we have to be confident we can distinguish these. To give an analogy, open meetings laws not only prevent conspiracies, they also lead to public trust in governance without all parties having to have blind faith. In any given meeting, the oversight imposed by meetings-laws may seem inconvenient or onerous, but in hindsight it cumulatively leads to a more efficient government because it is trusted. It must be possible to convince the losers of elections that they lost.

4) Elections may be audited to detect statistically significant election problems when detailed precinct, vote type and machine level election data are publicly released and analyzed with demographic data.

General recommendations

1) Voting technology is high technology; get expert advice of computer scientists who are known experts in voting systems who do not have any conflict of interest.

2) Because technology changes rapidly, legislation, RFPs, and State Election Plans should emphasize performance specification over configuration specification.

3) Every aspect of electronic voting and elections systems should be open to public surveillance.

Getting expert advice

We recommend forming a panel of experts to guide voting system requirements. In particular we can recommend any of the computer professionals who've been involved in designing and evaluating better voting and elections systems.[1] The advisory committee should be people with no conflict of interest.

Other documents are available with recommendations for voting systems.[2]

We recommend against solely relying on any advisors who advocate positions which are widely disputed in the computer security community.[3]

Ten essential system requirements for trustable electronic voting

1) The voting system shall produce a paper ballot, inspect-able by the voter at the time of voting, and secured at the polling place. The voter may spoil the ballot and re-vote if not satisfied that the ballot is correct. Spoiled ballots shall be retained at the poll, or their absence explained by polling officials (as done now). Performance requirements for ballots may include retention of the mark of voters for at least one year, ability to be optically-scanned, hand recount-able, and conveniently stored.

2) Voting system software shall be freely inspect-able by the public. Software will be available in both source code and binary format, without any non-disclosure agreements. By voting software we mean all components: configuration files, application, operating system, peripheral drivers, font files, and all firmware including video subsystems. Software may not be altered within 6 months prior to an election.

3) Vote storage formats, electronic and paper, shall either be non-proprietary or licensed under fixed and reasonable terms so that alternative vendors can produce compatible voting software and machinery. (See IEEE-1622)

4) Computer-oriented paper ballot encoding (such as a barcode or OCR) is very highly recommended. If used, 100% of paper ballots shall be machine counted and compared to the electronic ballot record if it exists. Additionally 1% of these shall be hand counted and compared in detail to the bar codes. Additionally, a bar code reader accessible to voters shall be available in every polling place so that voters may verify their own bar codes. All discrepancies will be published before canvassing and shall require a hand recount if sufficiently large.

---

[1] Known voting system design experts include Former ACM President, IBM ret Barbara Simons, Prof. Avi Rubin (Johns Hopkins), Prof. Dan Wallach (Rice U), Prof. Arthur Keller (UCAL Santa Cruz), Prof. Doug Jones (Iowa State), Dr. David Jefferson (Lawrence Livermore National Lab), Dr. Rebecca Mercuri (Harvard), Dr. David Mertz and Prof David Dill (Stanford).

[2] The new California draft-standards and laws may be a useful reference for Utah. Harvard University recently published an election systems best-practices guide, and a best practices document for optical scan voting machines is being developed by Charlie Strauss with other computer professionals.

[3] Prof. Ted Selker, Prof. Brett Williams, Prof. Glen Newkirk and Prof. Michael Shamos

5) If computer-oriented paper ballot encoding is not used (such as with hand marked optical scan ballots) mandatory randomly-selected surprise hand recounts shall be conducted of the voter-verified ballots in 3 percent of the jurisdictions immediately following each election. Half shall be selected after the elections on a random basis. Half shall be from nominations by the candidates. The Election office shall promptly publish the results of those recounts.

6) In the event of a sufficient discrepancy between any electronic record and the paper record, neither has primacy: a judge informed by experts will decide how to reconcile the difference on the basis of which is most likely to be correct under the specific circumstances in each case. Election officials themselves will not make the decision or establish a general policy mandating one form. However, in the absence of evidence to the contrary the paper ballots shall be preferred.

7) To protect the voter from intimidation and to prevent the selling of votes, the secrecy of the ballot must be preserved. Thus extreme administrative precautions shall be taken if roll-tape or time-stamped or serial-numbered ballots are employed since these preserve vote order. Similarly, electronic records that would enable reverse engineering vote order shall be avoided or administratively secured. Notably, if ballots reveal the voter's preferred language, precautions are needed to preserve voter privacy, since rare languages may indicate ethnicity or identity.

8) Further, ballot secrecy requires that absolutely no voter receipts — vote confirmation records taken home by a voter — shall be produced, including "secure" cryptographic records.

9) Absolutely no remote communications or networking of machines shall be permitted. All data ports on the machine shall be physically secured with tamper evident seals. (Exposed data cables should be armored.)

10) All vote and audit records as well as all ballot configuration files shall include standard good-practices such as checksums and digital signatures so that every file can be validated by any software reading it. This includes all vote processing software, not just the voting terminal software. If Computer-oriented paper ballot encoding is used, the paper ballots shall contain checksums and digital signatures.

Additional recommended best-practices

1) Legislation shall distinguish between ballot marking devices, ballot storage systems, ballot scanners, ballot counters, and ballot databases. Currently, these separate functions are somewhat conflated in law; they present different risks and can be secured in different ways.

2) The voting machine shall produce an audible ding (or flashing lamp or external equivalent notification) sufficient to alert both the voter and election officials whenever a valid paper ballot is produced. If a voter walks away without producing a ding or otherwise not depositing a ballot, election officials shall try to inform them a ballot has not been cast. The ding also

inhibits voters with stolen terminal activation cards from voting multiple times unobserved, or voters from failing to turn over spoiled ballots.

3) Audit logs shall not be alterable. All machine audit logs shall be written to nonvolatile, write-once media, signed by witnesses upon being physically secured in the machine with tamper evident seals. An example of this would be a paper tape or a write-once CD-R. Audit logs shall be published promptly.

4) To hold an election when a known software or hardware bug exists, the SOS shall identify the risk and countermeasures and each clerk shall certify that the countermeasures are in place. All bugs, countermeasures and certification shall be published before an election is canvassed.

5) Policies for coping with abnormal conditions such as printer malfunction or machine malfunction shall be established by the SOS prior to elections.

6) Parallel testing. At random on Election Day itself machines shall be selected and pulled from operation. Teams of testers will vote on the machines under conditions simulating election conditions and patterns (including environmental factors). These shall be video taped and the intended votes compared to the recorded votes with any discrepancies reconciled with the video.

7) To permit parallel testing on other than Election Day, it shall be a felony to intentionally design a voting system with a hidden means of estimating the true date beyond what is deliberately entered by an operator via a single portal. Examples of hidden alternate time keeping include: battery drain, IR light sensors, AC wall voltage, and the clocks of peripheral devices such as the graphics card or power management units.

8) It shall be a felony for any person to take a photograph of a voting machine for the purposes of spying, intimidation or vote-selling.

9) Sufficient voting machines to deal with 100% turnout and reasonable failure rates shall be available, allocated using statistically valid methods. Where the primary voting technology is a ballot marking device [page 3, item 1], alternate machine readable optical scan systems (paper ballots) shall be readily available in case of unpredictable 'surges' of voters or power failures.

10) Screen calibration shall be periodically validated throughout Election Day. Anomalies shall be logged. Line voltage shall be logged on Election Day.

11) If a voter re-votes, the previous ballot shall be spoiled both on paper and in the electronic record. To assure correspondence between the records, the voting system shall be designed to inhibit an electronic record from being spoiled once a voter has placed a paper ballot in the ballot box.

12) To allow a machine to securely self-witness its own data in a pristine state, before any electronic vote storage devices are removed from a machine or any device is connected to the machine after an election, the machine itself shall write the vote records to a write-once

non-volatile medium (e.g. CD-R, “FROG”) that was signed in advance by the election judges or other witnesses.

13) All software used by the machine shall be loaded into the machine memory from non-writable media physically secured inside the machine and not accessible to any poll worker. This could include CD-roms or hard disks or flash memory whose write-functions have been physically disabled. The media shall be encased in tamper evident seals and all randomly audited machines shall have the software-containing device audited to insure that the binary software matches the certified software.

14) All software and operating systems shall follow software design best practices. For example, all data records should be read into memory using a no-execute protocol available on modern CPUs, and any writable storage devices should be mounted using no-execute protocols. (In the event of a software error, no-execute protocols prevent accidental execution of portions of memory meant to store data and not programs.)

15) Despite all precautions, election problems may still occur due to hardware failures, electronic failures, innocent or malicious programming errors, mistakes made by election officials, ballot tampering or spoilage, mistakes made by voters, etc. If the data formats used for election data reporting and election setup are sufficiently transparent and are disclosed to the public, third-party tools can be developed that allow observers to independently verify election results. If we require the publication of all of the relevant election data, including the election configuration files and the raw precinct-level data, then we will extend, to election observers, considerable ability to detect and correct any election problems.

Charlie Strauss, voter@vvnm.org 505.663.0716 Verified Voting NM vvnm.org
David Mertz, Ph.D. mertz@gnosis.cx , Chief Technology Officer, Open Voting Consortium
Technical Editor, IEEE P-1622 (Voting Systems Electronic Data Interchange) http://gnosis.cx/voting/
Kathy Dopp, MS kathy@uscountvotes.org 435-608-1382 Utah Count Votes utahcountvotes.org

Many other computer professionals and voting activists reviewed and contributed to this document.

This document can be found on the Internet:
http://uscountvotes.net/voting_machines/Best_Practices_US.pdf