Frequently Asked Questions about DRE Voting Systems

David L. Dill, Rebecca Mercuri, Peter G. Neumann, and Dan S. Wallach

Section 1: Paper vs. Computers

- 1.1. What is a DRE?
- 1.2. Why are computer scientists upset by DRE voting systems?
- 1.3. What exactly is a "voter-verifiable audit trail" and why must we have it?
- 1.4. Then how can DRE vendors improve their systems?
- 1.5. If DRE systems have paper, then what's the point of the computer?
- 1.6. What if the paper and the computer disagree on the vote totals?
- 1.7. Won't the paper produced by such a computer be just as subject to problems as traditional punch-card or optical-sense systems?

Section 2: Software Quality

- 2.1. DRE vendors say their software has been thoroughly tested. Isn't that good enough?
- 2.2. DRE vendors claim that preserving the secrecy of their proprietary technology gives them an important hedge against being compromised.
- 2.3. The vendors have to escrow the source code of their systems with the Secretary of State's office. Doesn't this solve the problem?
- 2.4. Don't the Federal and State certification processes make sure the machines are secure?
- 2.5. Why are electronic voting machines different from your bank's automated teller systems?
- 2.6. Why are electronic election machines different from safety-critical systems with stringent requirements for reliability (for example, airplane flight-control systems)?

Section 3: Practical Advice

- 3.1. We are mandated to replace our existing voting system, but no existing replacement is certified for our use that does what you suggest. What should we do?
- 3.2. How great are the risks of using DRE machines?
- 3.3. How do these risks compare with systems based on
paper ballots?
- 3.4. Have problems in DRE machines been seen in real
elections?
- 3.5. What about accessibility for voters with disabilities?

Section 1: Paper vs. Computers

1.1. What is a DRE?

DRE stands for "Direct Recording Electronic" voting machine. As
the name suggests, the voter directly enters the votes, which
are recorded electronically. Almost all touch screen voting
machines are DREs, although there are other DREs that have
knobs or switches instead of touch screens.

1.2. Why are computer scientists upset by DRE voting
systems?

Computer scientists, as well as voters, are upset by paperless
DRE voting systems because we know that even a beginning
programmer can write code that displays votes one way on a
screen, records them another way, and tallies them yet another
way. This can happen for a variety of reasons, including
software and hardware errors, or "hacks" installed into the
voting machines. These problems can occur even when voting
machines have been thoroughly inspected and tested. DRE
systems experienced a number of problems already in the 2002
elections, and we see this only as the tip of the iceberg.

1.3. What exactly is a "voter-verifiable audit trail" and
why must we have it?

To have confidence that votes are being correctly recorded, we
need to guarantee that voters will directly see a physical object
that shows their vote. Voters must be confident that this
physical object cannot be thrown out or changed by the voting
system. Of course, once a vote has been cast, the voter's
anonymity must be preserved, and this physical object becomes
the final record of the voter's intent. The voter cannot keep any
proof of how they voted.

Traditional manual elections that use paper ballots and marking
pens, as well as newer optical scan systems (i.e., mark-sense or
bubble form), have the audit trail we want. Voters mark the
paper, can hold it in their hands, can verify it, and can then put
it in a ballot box. We also like DRE voting systems that print a
paper ballot which the voter can see and approve. Paperless
DRE systems tell voters to just "trust us" that the system will
work. That diminishes voter confidence.
1.4. Then how can DRE vendors improve their systems?

DRE voting systems need to use printer attachments to produce a printed paper ballot of the voter's selections, printed in the voter's native language. The voter can read and verify that his or her intent is represented on the paper ballot. The computer-printed paper ballot should be treated with all the care of traditional paper ballots. The ballots are, of course, anonymous, and election officials keep them securely in ballot boxes.

In a DRE system with a paper component such as this, the vendor's software no longer needs to reach unattainably high levels of quality and security, so long as it works well enough to produce the paper ballot. Either the voter is happy with the paper output or not. If not, then it's a spoiled ballot, and traditional procedures can be applied to guarantee that the voter's spoiled ballot is not placed in the final ballot box.

1.5. If DRE systems have paper, then what's the point of the computer?

Computer-based systems can offer significant improvements in human-factors, making voting accessible to voters with visual or motor impairments as well as supporting a number of different languages. DRE systems can help prevent undesirable over-voting and under-voting. They can also support elections with more races and even with non-traditional voting systems like approval voting or instant run-offs. Furthermore, the use of computers allows election workers to quickly tally computer-based voting records. However, the paper-based records will be more accurate and will need to be tallied as well.

1.6. What if the paper and the computer disagree on the vote totals?

If there is a difference between counts produced from the paper ballots and purely electronic counts from the voting machines, paper ballots should generally take precedence as the paper ballots have been seen and verified by voters, whereas the electronic counters inside the voting machines have not.

Of course, in the event that the election administration had problems (for example, misplacing paper ballot boxes), then the electronic counts may in such special circumstances be considered to be better than nothing at all from a given precinct. Whenever paper ballots exist, their tally will be the most dependable information available.

1.7. Won't the paper produced by such a computer be just as subject to problems as traditional punch-card or optical-sense systems?

Luckily, no. There will be no "chads" on the paper that need to
be punched and no bubbles for a voter to fill in. Computer printouts can be easily read, both by people and by other computers, providing two possible avenues for counting paper ballots. Furthermore, cryptographic techniques (i.e., secret computer codes) can be applied by the DRE system to make it essentially impossible for voters to insert fake ballots.

Section 2: Software Quality

2.1. DRE vendors say their software has been thoroughly tested. Isn't that good enough?

It is not enough to show that a system "seems to work." We know that the testing of existing DRE systems has already missed some impressive flaws. For example, Diebold voting systems in Georgia would "lock up" after a few hours use, despite being tested in a mock election with more votes than a typical machine got during the real election.

Second, testing for security problems, especially if they were intentionally introduced and concealed, is basically impossible. Consider the cute surprises inserted by programmers into commercial software that are triggered by obscure combinations of commands and keystrokes, called "Easter eggs." These routinely slip through vendor's quality assurance testing, including the amazing flight simulator that is hidden in Microsoft Excel '97. An Easter egg slipped into a voting program would never be detected. If the Easter egg allowed a voter to modify the votes inside the machine, it could change the whole election.

2.2. DRE vendors claim that preserving the secrecy of their proprietary technology gives them an important hedge against being compromised.

This argument is generally called "security through obscurity" and has been disproven time and time again. Adversaries will always be able to get voting machines to tear apart and study. They may even be able to design "hacks" that modify voting machines after the machines are in use.

Computer security researchers accept that, for a system to be secure, it must be designed to resist adversaries who know every detail about its inner workings. Furthermore, we have seen too many cases where a vendor claims its software is secure when it turns out to be full of holes. Currently, the results of voting system certification tests are kept secret and vendors hide their hardware and software from other independent scrutiny by aggressive use of trade secret agreements. Security claims need to be independently audited, and, even if the source code is not available in public, the detailed security audits should be public, to make a strong argument that the voting system actually works.
2.3. The vendors have to escrow the source code of their systems with the Secretary of State's office. Doesn't this solve the problem?

It doesn't seem to help at all. In fact, it's not clear that there are any circumstances where the code can be examined. In cases where clearly flawed elections have been challenged in some states, the vendors and courts have refused to let independent experts look at the source code. Furthermore, the detailed reports from the certification authorities have also been protected by trade-secrecy, so even in a court proceeding it is impossible to check whether the equipment has been properly configured, and whether testing has been sufficient to assure confidence in its accuracy and reliability.

2.4. Don't the Federal and State certification processes make sure the machines are secure?

A: No. The NASED (National Association of State Election Directors, the organization that oversees certification to Federal requirements) and California state certification processes are considerably weaker than other accepted standards for the security of computer-based products. Security-critical systems for the Department of Defense, for example, must meet the more stringent standards overseen by National Institute of Standards and Technology (NIST), such as the International Standards Organization (ISO)'s Common Criteria. Many other computer vendors, such as health care, voluntarily apply the NIST standards to their products, but to date, no electronic voting system has been certified under the NIST programs. (Some may have received ISO 9000 certification, but this is largely meaningless in the context of security.) The Help America Vote Act requires NIST work to develop a real standard (the FEC recommendations are not a standard, and require adoption by the states, only 2/3 of which have adopted) for voting systems, but this work has not yet been funded, so an enforceable US standard for design, construction, and testing of election equipment does not yet exist. All current (and for the forseeable future) voting product "testing" under the NASED program is paid for by the vendors, performed in secrecy, and detailed result reports are not released for public scrutiny.

2.5. Why are electronic voting machines different from your bank's automated teller systems?

The ATM systems have all sorts of internal auditing, and they provide you with a paper record of your transaction that you can verify on the spot. If there is a discrepancy, you can immediately go into the bank and have it resolved. If your monthly statement shows transactions that you never made, you can get your bank to fix them. ATM systems also include cameras that can be used to identify criminals or to prove that a genuine customer was using the ATM. Banking systems are not
anonymous, as elections are required to be. Also banks are insured for losses (and there are considerable losses at ATMs), while elections are not insured. Election systems are thus significantly more difficult to design and build than ATM systems.

In fact, serious security problems have recently been found with bank ATMs.

### 2.6. Why are electronic election machines different from safety-critical systems with stringent requirements for reliability (for example, airplane flight-control systems)?

The technical community is quite skilled at designing, building, testing, and evaluating computer systems that must operate within highly reliable safety-critical applications such as real-time aviation control, air-traffic control, space systems, healthcare systems, and so on. It adds significantly to the development costs, but those costs are generally justified by the clearly recognized dangers from having these systems fail. DRE voting systems are not built with anything approaching the level of care that goes into building safety-critical systems.

Furthermore, safety-critical systems are not generally designed to be secure against arbitrary misuse or tampering. Election systems need to have the auditing and double-checking features found in ATM systems combined with the reliability achieved in safety-critical systems. That's a tall order, and current DRE systems give us no reason to believe they achieve this. However, if DRE systems included paper ballot printing, as discussed above, this level of reliability would no longer be necessary.

### Section 3: Practical Advice

#### 3.1. We are mandated to replace our existing voting system, but no existing replacement is certified for our use that does what you suggest. What should we do?

The authors of this FAQ do not wish to endorse any specific vendors, although we do point out that both Avante's VoteTrakker system and Advanced Voting Systems/Hewlett Packard's voting system support voter-verifiable audit trails and are certified for use in California. If your municipality, perhaps in collaboration with other municipalities around the U.S., demanded these features, other vendors would certainly make them available in time to meet the March 2004 deadlines.

Major vendors Sequoia, Diebold, and ES&S have prototypes of voter-verifiable paper trails that can be attached to their DRE machines. These systems still need to be certified, but that could probably be completed in time for the 2004 elections.
3.2. How great are the risks of using DRE machines?

The risks of paperless DRE machines are large. Programming errors are an inevitable fact of life given current technology. With these paperless DRE machines, there is nothing that can stop a determined group from achieving large-scale election theft. We see no reason why major problems will not occur, including obviously messed up elections, election of incorrect candidates, and, certainly, disillusioned and disenfranchised voters.

*DRE voting systems that use voter-verified paper ballots have natural safeguards against numerous forms of fraudulent election behavior.* Current DRE systems have no such safeguards.

3.3. How do these risks compare with systems based on paper ballots?

Of course, election problems and outright election-rigging have occurred with systems based on paper ballots. However, good election administration can minimize these problems. People understand paper ballots and know what measures need to be taken to keep them secure. Wide-scale tampering with paper ballots is quite difficult.

Computer-generated paper ballots can be *considerably better* than regular paper -- barcodes and cryptography can be added to the ballot to ensure that the paper was produced at the time of the election, and to prevent ballot-box stuffing. Hence, a "better ballot box" can be produced through the combination of computers with paper. With paperless DREs, the risk of a large scale computer error or fraud that can globally affect the outcome of an election is high. With paper ballots, each voter will know that their ballot has been cast correctly, and controls can be put into place that will ensure that the tabulation is performed publicly and properly.

With paperless electronic voting systems, there is a real risk that bugs or security holes could affect large numbers of votes, regardless of how well the election is run otherwise.

In a well-run election, paper ballots are vastly more reliable and secure than paperless DRE machines.

3.4. Have problems in DRE machines been seen in real elections?

Yes! Problems are routine. Disturbingly, no one gets to the bottom of some of them, even when the outcome of the election may have been affected. Here is one of many examples: In March 2002, in the city of Wellington, Florida, there was a runoff election between two candidates for a single office. The final tally was 1,263 to 1,259, but 78 ballots had no recorded vote. Elections Supervisor Theresa LePore put forth the implausible
explanation that those 78 people came to the polls yet chose not to vote for the only office on the ballot.

Here is another example: In 2000, a Sequoia DRE machine was taken out of service in an election in Middlesex County, New Jersey, after 65 votes had been cast. When the results were checked after the election, it was discovered that, out of those 65 voters, no votes were recorded for the Democrat and Republican candidates for one office, even though 27 votes each were recorded for their running mates. A representative of Sequoia insisted that no votes were lost, and that voters had simply failed to cast votes for the two candidates. Since there was no paper trail, it was impossible to resolve the question.

These problems could have been avoided if the machines had printed voter-verifiable ballots. Voters would have caught missing votes when they inspected their paper ballots, and these ballots would have been available for counting when the election results were questioned.

### 3.5. What about accessibility for voters with disabilities?

See the Voting Accessibility Resources: Improving Voting Systems for Disabled People page.