The Dynamics of Counting and Recounting Votes

The limitations of current paper- and electronic-based voting systems and recount procedures can undermine the credibility of public elections. A corroborative, redundant voting system that performs vote counts via independent mechanisms at the polling place could address these shortcomings.

ALEC YASINSAC
Florida State University

MATT BISHOP
University of California at Davis

Accuracy is a key component of a fair election. A reliable voting mechanism must accurately capture the vote with a ballot that correctly reflects the voter's choice, as well as accurately count and tabulate the votes. The system must also accurately report the result, correctly declaring the winner. A system that fails to do any of these things can cause an overall error in election results.

Given how much a representative government depends on election results, voting mechanisms should be scrupulously crafted to ensure each election's accuracy. However, the US presidential election in 2000, for example, was an exercise in confusion; in some jurisdictions, voters found the ballots confusing whereas others had controversies about accurate tallies. This controversy, coupled with the desire to eliminate paper storage and provide better access, led to the US Help America Vote Act (HAVA). That act, and ancillary funding, led to the widespread deployment of electronic voting (e-voting) systems.

However, public discomfort levels in the US are rising, fueled by reports that the systems are susceptible to malicious manipulations by attackers ranging from rogue voters to corrupt election officials and vendors.[1,2] The controversy over e-voting systems masks the vulnerability of the entire election process, which by its nature is susceptible to deliberate or accidental manipulation. For example, in 2006, an audit of the Florida state voting rolls revealed approximately 80,000 duplicate voter registrations,[3] which could lead to a voter casting multiple votes. In 2000, an attempt to purge felons from Florida voting lists led to the state ordering the removal of voters erroneously identified as felons, including the election supervisor for Madison County.[4] Regardless of intent, this inherent inaccuracy undermines the integrity of the election process.

This article presents some issues with both paper and electronic ballots and focuses on scientific and engineering processes to improve voting precision, safety, and efficiency. Intuition suggests that computer-based electronic systems offer tremendous potential to provide vital accuracy and accessibility properties, though not without challenges. Similarly, paper-based systems have natural properties that can deter or prevent some types of integrity and security vulnerability inherent to electronic systems, but these too are not without problems. After discussing the strengths and weaknesses of electronic and paper ballots with respect to initial counts, we discuss auditing approaches to corroborate the initial reported results and propose protocols and procedures to strengthen the auditing mechanisms.

Election requirements and terminology

An election has many requirements. Accuracy is first and foremost; the final tally must reflect the voting of the voters. Although often stated as "counting the cast votes correctly," the requirement is broader. If a voting system prevents a voter from casting a legal vote, the results of the election will be inaccurate, even though the cast votes are counted correctly.

To be considered fair, an election must also be

credible, meaning the electorate must accept the results as legitimate. This adds two more requirements:

- *Verifiability.* The proclaimed results of the election must be verifiable. In essence, this means that we can recount the votes, verifying that the recount total agrees with the announced total. In addition, the auditor should be able to check that the only votes cast were by legal voters and that no legal voter was denied the opportunity to vote.
- *Transparency.* Any voter who wants to observe the election process can see everything except individual voters casting their vote. This also implies that the process is transparent to voters, so they can determine whether the election procedures are properly followed.

Confidentiality forms the basis for the two remaining requirements, which are related to preventing vote attribution:

- *Anonymity.* A third party must not be able to link a ballot to an individual. This prevents retribution should voters cast unpopular votes or not vote as a third party instructed them to.
- *Secrecy.* Voters shouldn't be able to prove to a third party how they voted. This prevents voters from selling their vote because the purchaser has no way to verify that the votes sold were actually cast.

In this article, we show how well various technologies meet these criteria.

Because terminology varies wildly, we present ours here. An *election system* consists of all mechanisms used to run an election. The *election management system* refers to management tools used to generate ballots, register voters, manage polling stations, and tally votes. The *voting system* captures the voters' votes on ballots, and it records and (possibly) produces intermediate tallies. Common voting systems are electronic computers (called *direct recording electronic*, or DRE, systems) with voter-verified paper audit trails (VVPAT), pencil and paper ballots, mechanical punches and cards, and mechanical lever systems. The *auditing system* validates the results. Common auditing schemes include a partial recount, such as California's legally mandated 1 percent recount, and a full recount when an election is disputed.

Demonstrably correct initial vote counting is critical to the success of voting systems, regardless of the auditing mechanisms in place. Auditing relies on information extracted from e-voting systems, and if that information is corrupted, so are the audit results. Because our focus is on the system, we assume that the voter is properly registered, that the user interface correctly captures the voter's intent, and so forth.

Paper-based voting systems

The traditional voting mechanism has voters mark a paper ballot to indicate their candidate preferences. Voters are comfortable with paper ballots—even though voters in general understand that paper-based voting systems aren't perfect, for most situations, they are suitably accurate and secure. Still, paper-based voting systems face inherent accuracy and security challenges; an obvious example is that they are vulnerable to human error and bias.

Counting ballots and human errors

Before mechanical cash-counting mechanisms were perfected, banks recognized that errors occurred when people counted money. To compensate for those errors, they created redundant processes in which tellers recounted cash bundles before attesting to their counts' accuracy. More rigorous procedures included other individuals recounting bundles of cash and comparing counts made separately. Still, human error occurs.

Ballots are inherently more difficult to count than currency. With cash, tellers separate and then count different denominations. Paper ballots contain more than one race per page, so it's rarely possible to separate ballots from different races. Each race might also have several candidates, so ballots might have pages of candidates in a single race. Thus, many pages might not have any vote marked, or the ballot might be overvoted with single votes on more than one page. (An *overvote* occurs when a voter casts more votes than are allowed. For example, if there are 10 candidates for three council seats, a voter might vote for four candidates.)

Like bank managers, election officials recognize these complexities and institute mitigating processes. Still, the opportunities for human error persist. Managers can do little to offset the differences in human performance. Regardless of the process, some people will count more accurately than others. Worse yet, some people will accurately implement the mandated counting procedures while others won't. Humans aren't machines and can at best simulate, not duplicate, machine precision.

VVPAT

The phrase *voter-verified paper audit trail* (VVPAT) implies that voters verified a paper representation of their ballot, and those representations will be used in audits. The term *audit* has many different meanings, and the meaning is crucial to understanding how elections use paper trails.

In standard computer usage, an audit is an analysis of information. For example, a bank audit analyzes transactions to determine if funds are properly handled. In voting terminology, we use the term to mean a verification that the reported election results are correct.

When we speak of a VVPAT, the assumption is that the paper trail provides a basis for auditing an election, thereby verifying that each vote is correctly counted. Unfortunately, a VVPAT does no such thing. The problem lies in the inability to bind an individual ballot to the voter who cast it. The results of counting the ballots can be audited, but not whether the ballots reflect the will of the voters who cast them. In this sense, the paper isn't a receipt because, unlike a receipt, the voter does not (and cannot) keep it because there is no way to associate an individual with that ballot.

Voting systems demand accuracy and security, and if they fail to meet these properties, so will the election.

As an example, consider a precinct-count optical scan (PCOS) voting system. Once a voter inserts his or her ballot into the scanner, there is no way to know whether the vote was recorded correctly. Moreover, once voters insert their ballots into the scanner, they lose any association with them. By law, each paper ballot must be indistinguishable from all other ballots, except for the specific voter selections. A real receipt associates a particular customer to a particular transaction, which violates the law.

An election process that uses paper ballots is vulnerable to malicious tampering. For example, stuffing the ballot box is a well-known form of election fraud. Because we can't serialize ballots, malicious parties might inject illegal ballots into uncounted bundles to affect the vote outcome or into previously counted bundles to affect recounts. Matching the number of voters to the number of ballots cast (called *voter reconciliation*) can mitigate this vulnerability, but malicious parties might remove ballots or manipulate voter counts to evade detection or manipulate the final tally itself. Procedures are only as good as the people who implement them, and election officials have committed voting fraud in the past.

One simple way to manipulate an election is for a third party, such as a poll worker, to mark ballots on which no vote is registered in a race before or after they are counted. Similarly, a malicious party with physical access to a ballot might mark a second choice in a close race to cause rejection of the now-overvoted ballot. Once again, well-known procedures can mitigate this threat, but it still remains.

One of the most common paper ballot threats is "lost and found" ballots. Poll workers occasionally misplace boxes of paper ballots before or after they are counted, thus affecting the result. This occurred in the 2004 Washington state governor's race, even though rigorous paper ballot protection processes were in place; the recovered ballots changed the election outcome.

Paper-based ballot systems have served our representative government effectively for centuries, but many factors are causing us to consider approaches to attain a more accurate, effective election systems.

Science and e-voting

No scientific examination has yet addressed the security properties of paper-based voting systems and election processes. Without solid data on how vulnerable these systems have proven, claims of one being less vulnerable than the other are opinion, not scientific fact.

Additionally, no scientific examination has yet addressed the security of combined paper and e-voting systems. This area requires considerable study before we can make scientific assertions about the security properties of classes of voting systems.

No analysis has yet addressed the difference between the number of constrained data items in paper and e-voting systems. The number of constrained data items is a simple integrity metric. Essentially, the more constrained data items there are, the more difficult it is to ensure their integrity. For example, in a paper voting system, each ballot is a constrained data item. In e-voting systems, the storage mechanism holding multiple ballots is a single constrained data item. A study of these constrained data items, and the points of vulnerability they raise in the different types of voting systems, would be illuminating.

A Brennan Center report on modeling threats for election processes provides a systematic argument about comparative security among paper and e-voting systems.[5] That report provides valuable insight into how elections can be stolen. However, the monolithic state-wide voting system model that they exercise does not reflect existing practice. First, most states use multiple vendors, so the single-vendor attack mode is unlikely to affect an entire state; rather, it would only affect jurisdictions that use the compromised system. Additionally, most states allow voting by mail on demand, and this trend is increasing. This diminishes the impact e-voting machines can have because the number, and percentage, of voters that use them decreases. These two factors create a heterogeneous system that increases the ability to statistically identify electronic, or nonelectronic, voting mischief.

Notwithstanding these omissions, the report's greatest pitfall is its failure to examine the vulnerability of voting systems after an election, particularly the threat and risk exposure that occurs during the recount process.

E-voting system vulnerabilities

The main difference between paper- and electronic-based voting systems is the magnitude of the damage

that one person can inflict in a short time. Theoretically, sophisticated intruders might systematically alter e-voting systems to deny service or add, change, or delete large numbers of votes to affect an election's accuracy. In the past few years, several scientists have constructed attacks against certified e-voting systems that validated these threats.[6,7]

For example, in 2004, Tadayoshi Kohno and his colleagues identified and documented software flaws that could allow fraud in a certified e-voting system by a prominent voting system vendor.[8] Other tests and reviews confirmed these faults and identified others.[1,2] And in 2006, Edward Felten of Princeton and his students[9] demonstrated several attacks that even marginally sophisticated intruders could run in seconds, with little risk of being caught or even of leaving traces of the attack.

Software engineering

These attacks reflect a two-pronged challenge: first, the difficulty of removing all software flaws from any nontrivial program (software correctness) and, second, ensuring that the desired software is the running version (software attestation).

The first is a well-known issue of program correctness and robustness, and the second is a classic computer science computational problem. The software engineering discipline approaches program correctness and robustness through rigor and process-oriented approaches, often relying on heuristics. In fact, software engineering recognizes that projects differ significantly based on human factors. Thus, many traditional engineers question whether software engineering is really an engineering discipline. Traditional engineering ultimately results in a physical artifact such as a bridge. Software, in development and in its finished state, is invisible. Moreover, software engineering processes don't yet provide results as predictable as traditional engineering. In fact, Rice's theorem[10] says that, for every nontrivial property, the question of whether a given program satisfies that property is undecidable.

Software engineering has developed sets of well-known principles and processes, but it is evolving slowly. This situation is analogous to the way e-voting systems evolved. HAVA dictated voting system improvements, but e-voting systems had not yet matured. The systems were developed with inadequate software engineering processes, and vendors' concerns with time to market, core functionality, and market share left little time to focus on security.

Development methodologies that give confidence that a system will meet its requirements are essential to providing systems that provide correct initial counts, and the evidence needed to demonstrate that the count was correct. In one sense, HAVA funding guaranteed that any delivered voting software would not be secure because the initial funding level was not nearly enough to offset the costs of rigorous engineering. Security received less attention in the design and implementation, and the impact of the resulting vulnerabilities took time to emerge.

Because voting systems demand greater assurance than non-mission-critical systems, they're more expensive than normal systems. Voting systems demand accuracy and security, and if they fail to meet these properties, so will the election. Developing mission-critical systems requires the application of high-assurance techniques. These systems must incorporate features not normally included in other systems (such as redundancy, validation mechanisms, and fail-safe controls), so they require a rigorous development process.[11]

Recount complexities

An old adage asks why we have time to do it over, but we don't have time to do it right the first time? This is usually said about organizations that refuse to implement best practices, repeat mistakes, and fail to use well-known successful approaches, but instead rely on their ability to "fly by the seat of their pants." This approach undermines elections' credibility. With the stability of the government in the balance, elections must get vote counts right the first time.

This raises an interesting question. Suppose an election declares John the winner. A recount determines it was Paul. That Paul is now declared the winner has nothing to do with the recount being more accurate than the initial count. Paul wins simply because the law says the result of the recount supersedes the result of the original count. If a second recount produces a different result, then the result of the second recount overrides that of both the initial count and first recount. So, which result is accurate?

Recount impact

There are many advantages to resolving election winners on the first count. Besides the added expense, recounts that produce different results without a convincing explanation for the differences reduce constituents' confidence in the legitimacy of the election's result.

The following two examples support this thesis. In one county, when punch cards and an electronic tabulator were in use, election officials discovered after the election that the order of the names of the candidates differed between the punch cards that voters voted on and the tabulating machine. Consequently, the election officials notified both candidates and the press and conducted a public, hand recount of all the ballots with that race on it. As a result, a new winner was declared. Because the election officials provided a detailed explanation of the problem that caused the error

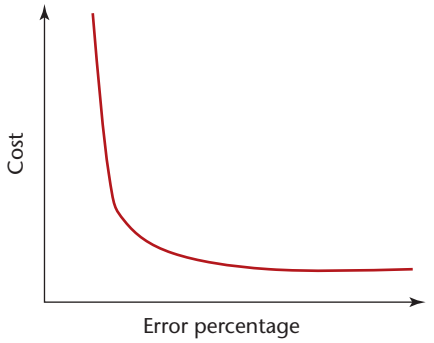

Figure 1. Voting system cost-accuracy curve. The goal of the voting process is to move the curve to the left, decreasing error while minimally increasing cost.

and conducted the recount in front of the press, other impartial observers, and the candidates' representatives, the result of the recount was accepted as correct and credible by all (not happily, in some cases).

As a counterpoint, consider the 2000 US presidential election results in Florida. The substantial questions about the initial results' accuracy led to multiple full and partial recounts in various jurisdictions throughout the state. Election officials gave little or no explanation of differences beyond human error. Many people felt this explanation was not credible and thought that partisan politics tainted the recount process, thereby making the results of the recount no more credible than the original results.

Clearly, recount procedures must be at least as accurate and secure as voting procedures and systems. If the recount result differs from the initial result, both results are called into question. Even in the face of a strong explanation for the difference, there is no way to prove which correctly reflects the votes cast—if either. Further recounts might only complicate the problem, as one gubernatorial election in Washington state demonstrated.[12]

Going further, the law of averages dictates that the candidate that received the most votes on the first ballot is statistically more likely to gain more votes in a recount.[13] If the counts differ, we can ask whether the same type of problem that caused votes for the winner to be missed could also have caused votes for the loser to have been missed. This means the difference in counts creates the credibility problem, not the difference in the declared winner (if any).

Also, if the original voting procedure is flawed, it might be impossible to demonstrate that a result is in fact correct (or incorrect). As an example, there is no way to precisely determine a voter's interactions on a DRE system unless a process is set up to capture those interactions. Certainly, voter actions are currently the most precise mechanism for determining voter intent, but paper trails don't contain sufficient information to capture every interaction. Hence, auditors can't derive this information from the paper trail, and so they currently conduct their audit without complete information.

Similarly, lost, destroyed, inserted, or manipulated paper and electronic ballots result in incomplete or inaccurate audit information. Moreover, delaying an audit provides greater opportunity for manipulating, changing, and otherwise altering the sources on which the audit rests.

This raises an immediate question. The focus of using e-voting systems in a trustworthy manner has been on providing data that enables effective audits (such as VVPATs). An equal, or greater, focus should be placed on designing and building systems that count votes accurately initially. The research community has placed some emphasis on capturing the voter's intent correctly[14] and has examined how to design better voting and audit systems[15,16] These studies all deal with various levels of assurance in the design and construction of the voting or auditing systems. These systems are not distinct. D. Sandler and Dan Wallach come closest to what we advocate; they focus on the auditing aspect, whereas we emphasize the data being audited.[17]

We conjecture that the primary consideration is cost. With paper ballots, the count and recount procedures are almost identical, so adding assurance to one adds assurance to the other. With electronic ballots, the procedures are different, one relying on an electronic tally and the others relying on the hand counting of VVPATs. The more careful the (re)counting, the more effort it takes. This suggests the curve shown in Figure 1.

Recount threat

Recounts provide opportunities for attackers to alter election results by trumping the initial result. Suppose Smith beats Jones by 3,500 votes. An attacker now knows how many votes must change for Jones to win. The Brennan Center report points out that retail or point-of-sale attacks that cannot affect a large number of ballots are unlikely to swing a statewide election, but their work is confined to retail fraud before the initial count.[5]

Given access to the jurisdiction's voting records, and knowing how many votes must be switched, an attacker could change the results of a close election by retail fraud. So knowing how many votes must be switched and the interval of time during which they can be switched enhances the opportunity of attackers to compromise the election with a greater likelihood of success and a lesser likelihood of detection.

Election fraud is a serious criminal offense. Anyone committing it risks grave consequences, includ-

ing incarceration and stiff financial penalties. To do so before the outcome is known is particularly risky given that the penalties are no less if the fraud merely increased the margin of victory or decreased the margin of loss. But attackers who know the election result know whether they need to launch an attack at all. Thus, knowing the election result is an important property for assessing the likelihood of fraud.

Also, knowing the election result tells attackers the minimum number of votes that they must change. For example, consider the 2004 Washington governor's race, in which the election night result was overturned after two recounts, amid claims of ballot stuffing and destruction.[18] The original result reflected a 261 vote margin out of 2.9 million ballots cast. A machine recount (that rejected some originally counted ballots and injected some previously uncounted ballots) reduced the original winner's margin to 42 votes. A second recount, this time by hand (with additional ballot additions and deletions), reversed the election and placed the new governor in office by a 129 vote margin. Our point is that, at most, it would only have been necessary to change 131 votes to change the result at any point during the recounts.

Whether fraud occurred, this situation was ripe for manipulation. Finding previously uncounted ballots, editing under-votes, and over-marking valid votes are three simple but effective count manipulation strategies when the adversary knows the number of votes needed, particularly when only a few votes can change the outcome. Moreover, paper ballots didn't preclude these irregularities, and they didn't inherently ameliorate this threat.

Limitations of the auditable paper trail

The goal of an auditable paper trail is to provide assurance that votes are recorded and counted accurately. However, studies have shown that many voters don't check the paper trail before casting their vote,[19] and when they do, they aren't likely to detect variations between their original selection and the paper record.[20] Thus, it would be more correct to say that auditable paper trails provide the potential for checking that votes are recorded accurately. There's no way to check that voters have in fact verified their own paper trail. After-the-fact verification would require that the voter be associated with the ballot in some way, thereby violating the ballot's anonymity and secrecy.

For example, someone could inject prefabricated paper trails or remove paper trails to affect the recount results. This requires tracking the paper. If each paper record of each voter's ballot could be traced to a specific voter, we could prevent adding ballots to or removing ballots from the paper audit trails. But, privacy is still a central tenet of fair elections, so integrity must be ensured without going back to the source after the fact.

Paper ballots suffer from these problems as well. Given that paper audit trails are usually on special-purpose (thermal) paper, paper ballots might be easier to forge than paper audit trails. The maturity of desktop publishing and the widespread availability of printers and scanners exacerbate this problem. An after-the-fact audit relying on paper might be counting paper that wasn't present during the election, or might not recognize that paper present during the election has been removed before the recount—for both paper ballots and audit trails.

Finally, existing e-voting systems print VVPATs on spools of paper similar to cash register receipts. This paper is awkward at best to review and count. A recent set of experiments in which two races from a spool of 120 ballots were manually reviewed resulted in only 57.5 percent of the subjects obtaining the correct result[21]—a finding that bodes ill for the use of VVPATs in auditing election results.

Recount verification fallacy

An additional argument for retaining paper ballots is the contention that count verification is essential to voter confidence, and that paper ballots allow this verification. Election officials conduct a recount to verify the first count. Such corroboration is a well-understood evidentiary concept in which an independent assessment that agrees with the original outcome confirms the original outcome's validity. However, a vote recount only corroborates when it agrees with the original count. Any difference in the counts diminishes both counts' credibility.

In evidentiary proceedings, when prospective corroboration contradicts the original information, each is weighed equally. Each establishes a reasonable doubt of the other. But in vote recounts, the last count determines the winner, without further corroboration.

Because vote recounts are imprecise, they rarely exactly match original counts. The problem is that the comparison is based on who wins, not the vote totals. So the recount is judged to confirm the original count if it reports the same winner. But the recount doesn't measure the winner; it measures the vote totals of the candidates that determine the winner. The claim that a machine recount just recycles earlier results is really a plus. If the count were right the first time, it should be identical every time it is checked.

These factors lead us to question the classic three-tiered vote recount system, in which a hand recount confirms or contradicts a machine recount that confirmed or contradicted the original vote count. There are no theoretical or scientific principles that suggest that a recount is more accurate than the original count. Moreover, recounts inject imprecision and intrusion opportunity.

Worse yet, the three recount tiers aren't actually

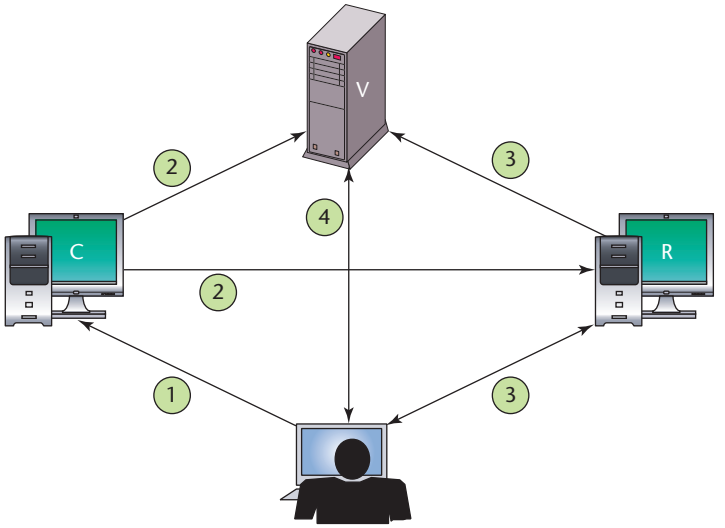

Figure 2. Corroborating vote count. The caster, verifier, and reconciler work together to record and verify the voter's choice. In this way, vote corroboration occurs in the polling place without the need for paper records.

recounts because the people involved in the counting and recounting add and omit votes at different stages in the process, based on their interpretation of the law and on other factors (such as discovered ballots and court orders). Vote error analysis is subject to bias and human error.

Corroboration results only from independent analysis of the same data. Corroborative mechanisms that use the results of earlier comparisons or that analyze different results or processes simply don't corroborate.

Corroborative, redundant voting systems

Consider a voting paradigm in which vote corroboration occurs when the original vote is cast. In such a system, independent vote counts occur via independent mechanisms at the polling place when voters cast their ballots. In such a corroborated voting system, there are three independent electronic voting components: caster, verifier, and reconciler. The voting process proceeds as follows:

1. Voters engage the vote caster, review the candidates, casts their ballot, and review and confirm their selections on the screen before committing their votes.
2. The vote caster records the votes and then transmits them to the reconciler and the verifier (such as via write-once media or hard wire).
3. The verifier displays the votes to each voter, who confirms and commits the selection; the verifier then sends the votes to the reconciler.
4. The reconciler compares the records from the vote caster and reconciler. The reconciler displays the reconciliation to each voter. If the totals match, the voter commits the vote. Otherwise, the voter notifies a poll worker and the process restarts.
5. When the voter commits, the vote caster, scanner, and reconciler accumulate the votes, and the voter leaves the polling booth.

Figure 2 illustrates this process, which leaves three separate, independent sets of electronic votes and vote accumulation records. This scheme has the voter verify directly the external representation of the vote's three copies. This protocol provides voter verification and triple redundancy while allowing audits to the voting station level, all without retaining any paper records.

Clearly, attacks could undermine the security of this process, and issues of composability and software assurance will be paramount. This process is an example of an architecture with three independent mechanisms that resist attacks on a single point of failure. Thus, it forms a strong foundation for potentially effective, attack-resistant e-voting.

Improving the quality of vote casting and counting on the front end is a must, else back-end auditing won't provide the necessary electoral accuracy and confidence. However, we can simplify auditing and multiply its impact by building it on a strong foundation. To achieve this result, we must examine the fundamental integrity, security, and composability properties of electronic- and paper-based voting systems, and we must rigorously analyze and exercise the solutions that emerge, focusing on the strength of their first-count properties. □

References

1. D. Wagner, D. Jefferson, and M. Bishop, *Security Analysis of the Diebold AccuBasic Interpreter*, tech. report, Voting Systems Technology Assessment Advisory Board; www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf.
2. H. Hursti, "Security Alert: May 11, 2006, Critical Security Issues with Diebold TSx," Black Box Voting, www.blackboxvoting.org/BBVtsxstudy.pdf.
3. B. Cottrell, "Auditor's Study Finds Problems in Voter Database," *Tallahassee Democrat*, 21 Jun. 2006.
4. G. Palast, "The Wrong Way to Fix the Vote," *Washington Post*, 10 Jun. 2001, p. B01.
5. *The Machinery of Democracy: Protecting Elections in an Electronic World*, tech. report, Brennan Center Task Force on Voting System Security; www.brennancenter.org/dynamic/subpages/download_file_36343.pdf.
6. A. Yasinsac et al., *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware,*

Final Report, tech. report, Security and Assurance in Information Technology Lab., Florida State Univ., Feb. 2007; http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf.
7. R. Gardner et al., *Software Review and Security Analysis of the Diebold Voting Machine Software*, tech. report, Security and Assurance in Information Technology Lab., Florida State Univ., Jul. 2007; http://election.dos.state.fl.us/pdf/SAITreport.pdf.
8. T. Kohno et al., "Analysis of an Electronic Voting System," *IEEE Symp. Security and Privacy*, IEEE CS Press, 2004, pp. 27–40.
9. A.J. Feldman, J.A. Halderman, and E.W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine," Center for Information Technology Policy and Dept. of Computer Science, Princeton Univ., 13 Sept. 2006
10. H.G. Rice, "Classes of Recursively Enumerable Sets and Their Decision Problems," *Trans. Amer. Mathematical Soc.*, vol. 74, no. 2, Mar. 1953, pp. 358–366.
11. A. Yasinsac and J.T. McDonald, "Foundations for Security Aware Software Development Education," *Proc. 39th Ann. Hawaii Int'l Conf. System Sciences Track 9,* IEEE CS Press, 2006, p. 219c.
12. "Judge Upholds Washington Governor's Election," *USA Today*, 6 Jun. 2005.
13. B. Harris, "Election Recounting," *The American Statistician*, vol. 42, no. 1, Feb. 1988, pp. 66–68.
14. K.-P. Yee, "Extending Prerendered-Interface Voting Software to Support Accessibility and Other Ballot Features," *Proc. Usenix/Accurate Electronic Voting Technology Workshop*, Usenix Assoc., 2007; http://usenix.org/events/evt07/tech/full_papers/yee/yee.pdf.
15. N. Sastry, T. Kohno, and D. Wagner, "Designing Voting Machines for Verification," *Proc. 15th Usenix Security Symp.*, Usenix Assoc., 2006, pp. 321–336.
16. J. Aslam, R. Popa, and R. Rivest, "On Estimating the Size and Confidence of a Statistical Audit," *Proc. Usenix/Accurate Electronic Voting Technology Workshop*, Usenix Assoc., 2007; http://usenix.org/events/evt07/tech/full_papers/aslam/aslam.pdf.
17. D. Sandler and D. Wallach, "Casting Votes in the Auditorium," *Proc. Usenix/Accurate Electronic Voting Technology Workshop*, Usenix Assoc., 2007; http://usenix.org/events/evt07/tech/full_papers/sandler/sandler.pdf.
18. K.-P. Yee, "Prerendered User Interfaces for Higher-Assurance Electronic Voting," *Proc. Usenix/Accurate Electronic Voting Technology Workshop,* Usenix Assoc., 2006; http://usenix.org/events/evt06/tech/full_papers/yee/yee.pdf.
19. R.G. Saltman, "Independent Verification: Essential Action to Assure Integrity in the Voting Process," no. SB134106W0703, US Nat'l Inst. Standards and Technology, Aug. 2006; http://vote.nist.gov/SaltmanRpt20060815.pdf.
20. T. Selker, "Testimony on Voter Verification: Presentation to Senate Committee on Rules and Administration," working paper # 31, Voter Technology Project, 2005; www.vote.caltech.edu/media/documents/wps/vtp_wp31.pdf.
21. S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," *Proc. Usenix/Accurate Electronic Voting Technology Workshop*, Usenix Assoc., 2007; www.usenix.org/events/evt07/tech/full_papers/goggin/goggin.pdf.

Alec Yasinsac *is a cofounder and co-Director of the Security and Assurance in Information Security (SAIT) Laboratory at Florida State University. His research interests include secure software, security protocols, and electronic voting. Yasinsac has a PhD in computer science from the University of Virginia. He is a senior member of IEEE, the IEEE Computer Society, and the ACM.*

Matt Bishop *is a faculty member in the Department of Computer Science at the University of California at Davis. His research interests include vulnerabilities analysis, network security, data sanitization, and electronic voting, and he is interested in improving education in secure and robust programming and computer security in general. Bishop received his PhD in computer science from Purdue University. He is a member of the ACM, the IEEE Computer Society, and Usenix.*