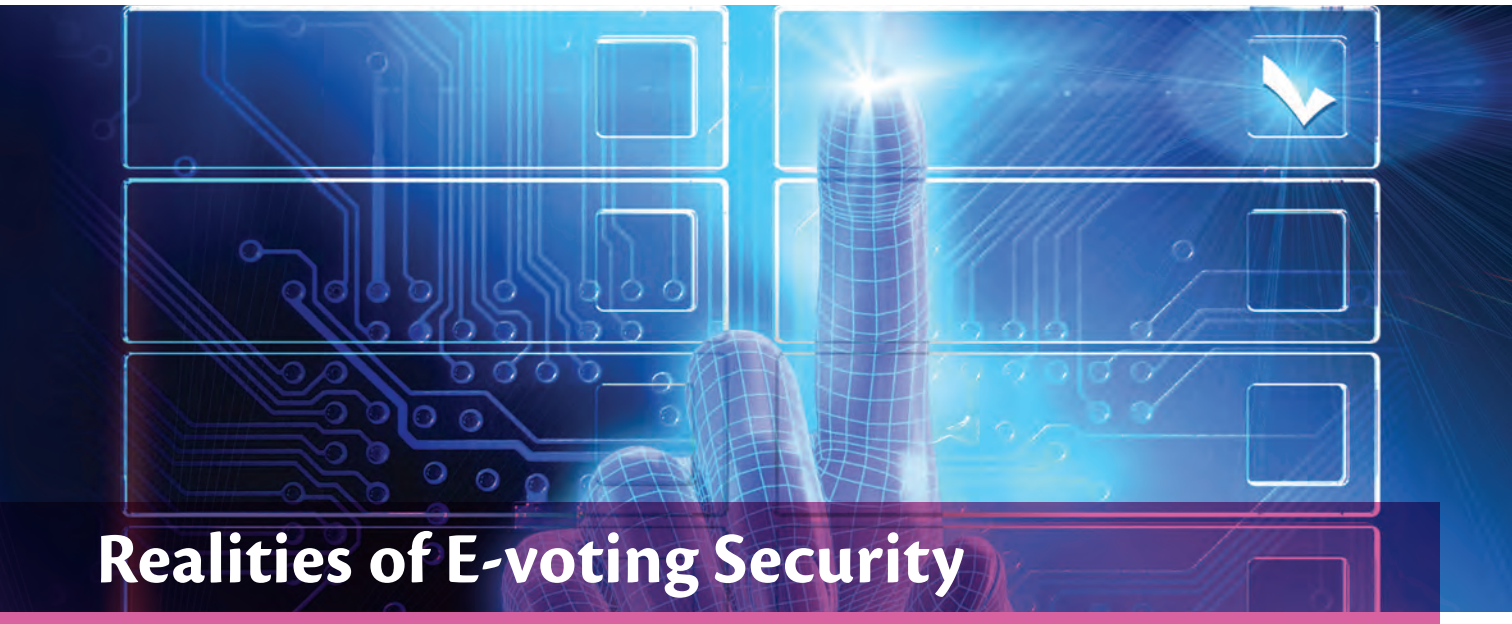

Realities of E-voting Security

Michael Shamos | Carnegie Mellon University
Alec Yasinsac | University of South Alabama

Electronic voting has been around since the 1970s, but until the US's 2000 Gore-Bush presidential election, it was largely out of the public eye. After the Florida punched-card debacle, it became clear that our election infrastructure needed renovation. The Help America Vote Act of 2002 mandated a solution of sorts, making US$3 billion available to states to move away from their long-lived, well-understood voting processes in the name of election accuracy. Soon thereafter, e-voting came under tremendous scrutiny for its potential to improve electoral precision as well as for its potential security pitfalls.[1]

Election Accuracy

If provably conducting the voting process with 100 percent accuracy were possible, we'd have little need for rigorous election auditing approaches. Unfortunately, election accuracy can't be guaranteed. In fact, most experts agree that competing priorities, such as privacy and transparency, create problems of proof that can't be overcome in real elections. Moreover, because the vast majority of elections have been decided by substantial margins, perfect accuracy hasn't been a practical priority.

The 2000 US presidential election brought this issue into sharp focus; its process wasn't sufficiently precise to confidently distinguish a winner under the rule of law. Many similarly close elections have since been in the news, such as Washington State's 2004 gubernatorial race, Florida's 2007 US Congressional District 13 election, and Minnesota's 2008 US Senate contest.

Possibly owing to increased funds available for elections, advanced polling, and campaign targeting approaches, or the rise of real-time news and social networking, elections with razor-thin margins are increasingly common, and methods to resolve close contests are receiving significant attention and debate. Unfortunately, if the winning margin is very small (say, less

 Copublished by the IEEE Computer and Reliability Societies

than 0.1 percent), no voting system can be relied on to reveal the true winner. Much of the argument about e-voting boils down to how large the margin must be to achieve trustworthy results.

E-voting was intended to enhance accuracy and speed the counting process. The hope was that improved user interfaces and computational reliability could eliminate human error and bias from the voting process. Widespread implementation of direct-recording e-voting systems aimed to prevent a repeat of the divisive Gore-Bush resolution process and narrow the attack surface created by postelection processes. Some states outlawed postelection access to voting materials, hoping to improve electoral accuracy by minimizing postelection mischief but, in doing so, hampered the audit process.

Election and Postelection Processes

Close contest resolution arguments generally take two approaches. The first focuses on processes, procedures, and algorithms that ensure the first count's accuracy, and the second focuses on infrastructures for postelection review and error identification. The four articles in this special issue address these two approaches. Two articles focus on algorithms that can provide inherent voting integrity (Aleksander Essex and Urs Hengartner's "Hover: Trustworthy Elections with Hash-Only Verification" and Richard Buckland and Roland Wen's "The Future of E-voting in Australia"), and two discuss post–voting period audits (Philip B. Stark and David A. Wagner's "Evidence-Based Elections" and Mark Lindeman and Philip B. Stark's "A Gentle Introduction to Risk-Limiting Audits").

Postelection audits have substantial appeal because they can increase both election accuracy and transparency. A negative side effect of audit-verified elections is that election officials might reduce focus on election day accuracy if their plan is to resolve close elections using audits. In addition, because audits are based on electoral artifacts, imprecision in election operations inherently reduces an audit's ability to identify and correct errors.

At best, audits are merely a check on processes and artifacts. They can uncover flaws in the election but, by themselves, don't correct the flaws. They might even reveal that no correction is possible, for example, if it's determined that more voted-but-uncounted ballots were lost or destroyed than the reported margin of victory. At worst, audits can introduce inaccurate or misleading information that might reverse a legitimate result. In addition, introducing or emphasizing the audit trail expands the attack surface for those inclined to nefariously influence the electoral outcome.

After three decades of incremental research advances, voting processes designed for inherent integrity have finally made their way into the marketplace and polling booth. Generally known as *cryptographic voting systems*, their automated precision and mathematically provable properties appeal to scientists but are difficult for voters and election officials to fully understand.

An important distinction between focusing on accurate election processes and audit-focused elections is the impact on voter confidence. For the former, election officials engineer and promote their election processes as "absolutely" accurate and sufficiently precise to minimize the need and, in some cases, the opportunity for review. Some states use regulation or legislation to limit access to electoral artifacts after the election is complete, slanting the resolution process toward accepting election day results. With audit-based elections, the resolution process is necessarily extended, sometimes by months. It might also offer a broad array of subjective, divisive processes, particularly when voter marking or other human error comes into play. Regardless of the trade-offs, rigorous election auditing is in a growth stage, and understanding its techniques and foundations is important in perpetually evolving election processes.

In addition to these four articles, a roundtable brings together security experts to examine e-voting security 10 years after the Help America Vote Act.

We would be remiss if we failed to emphasize that elections are complex processes, with myriad interacting, important parts. One negative result of the divisive 2000 US presidential election is the intense focus on the voting process to resolve close elections, when many other factors are equally relevant. For instance, no voting system can produce a confidently accurate result unless all, and only, eligible voters are granted proper access to the polls, an issue that has arisen again recently with the passage of strict voter ID laws. Voting is just one step in the electoral process and is no more or less important than any of the others.

The articles in this issue address various approaches to improving voting process integrity, which can help ensure electoral integrity and increase confidence that selection of our public officials is the citizens' decision. ■

Reference

1. T. Kohno et al., "Analysis of an Electronic Voting System," *IEEE Symp. Security and Privacy*, IEEE CS, 2004, pp. 27–40.

Michael Shamos is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University. Contact him at shamos@cs.cmu.edu.

Alec Yasinsac is professor and dean of the School of Computing at the University of South Alabama. Contact him at yasinsac@southalabama.edu.