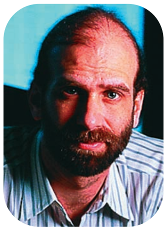
Voting Security and Technology



Bruce Schneier
Counterpane Internet Security

Voting seems like the perfect application for technology, but actually applying it is harder than it first appears. To ensure that voters can vote honestly, they need anonymity, which requires a secret ballot. Through the centuries, different civilizations have done their best with the available technologies. Stones and pottery shards dropped in Greek vases led to paper ballots dropped in sealed boxes. Mechanical voting booths and punch cards replaced paper ballots for faster counting. Now, new computerized voting machines promise even more efficiency, and remote Internet voting promises even more convenience.

An ideal voting technology would have four attributes: anonymity, scalability, speed, and accuracy—a direct mapping from voter intent to final tally. But in the rush to improve the first three attributes, accuracy has been sacrificed. All voting technologies involve translating the voter's intent in some way, many of them multiple times. And at each translation step, errors accumulate.

This is an important concept. Accuracy is not measured by how well the ballots are counted; it's how well the process translates voter intent into properly tallied votes. Most voting problems are a direct result of translation errors. For example, a punch-card system has several translation steps: from voter to ballot to punch card to card reader to vote tabulator to centralized total. Errors can occur in the system at each step—voters can be confused by the ballot's layout or improperly punch them (remember hanging chads?). Tabulating machines can malfunction. Ballots can be lost and not counted. Ballot subtotals can be misplaced and not counted in the final total.

The solution is simplicity. The fewer the translation steps, the fewer errors. Handwritten ballots are simply more accurate than computerized systems because there are fewer translation steps. Many European countries use paper ballots. But Europe doesn't hold dozens of different elections on the same day, as the US does. And Europeans don't demand final results before bedtime on election day, as do US citizens. Paper ballots might win on accuracy, but they fail on scalability and speed.

So, if it's technology to the rescue, we must recognize the potential for errors—both accidental and intentional—in their controlling software. Problems with computerized systems are almost cliché by now; people are even talking about the possibility of wholesale fraud.

Because elections happen simultaneously, there is no means of recovery if a problem is detected. Imagine if, in the next presidential election, someone discovered problems in the election machines in New York. Would we let all of New York vote again in a week? Would we redo the entire national election? Would we tell New Yorkers that their votes didn't count?

My suggestion, echoed by many computer-security experts, is a computer voting machine that prints out an ATM-style paper ballot. The voter checks the paper ballot for accuracy and then drops it into a sealed ballot box. The paper ballots are the "official" votes and can be used for recounts, while the computer provides a quick initial tally. E-voting machines must have the ability to verify some of the translation steps; voters can then verify that the machine correctly recorded their votes, and election officials can, if there is a recount, verify the votes were correctly tabulated. We can't eliminate translation steps, but we can add redundancy.

Even with a system that includes a paper ballot, we need to realize that the risk of errors and fraud cannot be brought down to zero. It's a myth that elections are accurate to the single vote. University of Cambridge professor Roger Needham once described automation as replacing what works with something that almost works, but is faster and cheaper. We need to decide what's important, and what trade-offs we're willing to make to get it. □

__Bruce Schneier__ is one of the world's foremost security experts and Counterpane Internet Security's chief technology officer. His new book, Beyond Fear: Thinking Sensibly about Security in an Uncertain World, *was published in September 2003. Contact him at www.schneier.com.*