By Anthony Di Franco, Andrew Petro, Emmett Shear, *and* Vladimir Vladimirov

Small Vote Manipulations Can Swing Elections

Considering the effects and implications of changing only a single vote per machine.

Under the mandate of the Help America Vote Act, precincts across the U.S. are upgrading their polling processes. Some precincts are choosing to purchase electronic voting machines, and some commentators advocate using e-voting machines as the standard. The use of direct-recording electronic voting machines (DREs), or more generally, any electronic means of vote tabulation and reporting, raises the concern that a single, simple, subtle fraudulent change to the system software can take effect everywhere these machines are deployed.

We attempted to determine the influence a hypothetical adversary might have had on the outcome of the 2000 U.S. Presidential election. Our adversary is able to select and change a small fixed number of votes per machine, representing the effect of modifying the voting software to misreport the results from each machine. A seemingly insignificant action on every voting machine, multiplied by the large number of machines required across the country, gives the adversary considerable influence. We calculate the number of states and electoral votes such an adversary might change, and conclude that the outcome of the election can be changed by manipulating one vote per voting machine. Furthermore, changing a few more votes can establish, or overcome, a considerable margin of victory.

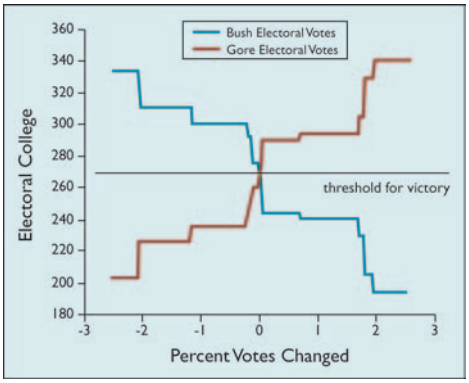
Method

We examine a hypothetical electronically balloted version of the 2000 election, assuming that 90% of the total votes are cast by means of e-voting machines. The remaining 10% are assumed to be cast in some other way (hand-counted paper ballots, lever machines, and so forth) and do not contribute to the number of e-voting machines required. In essence, we ask: What if e-voting advocates [9] succeed in making DREs universal?

We suppose an adversary favoring candidate B who selects from each voting machine m ballots containing votes for candidate A and changes them to votes for candidate B. We then assume one e-voting machine is required for every v votes to be cast by machine. The number of voting machines required is thus (90% × total votes cast) / v. We use

v = 200 in our calculations. We believe this is reasonable given the recent e-voting machine purchases of the states of Georgia and Maryland.[1] A voting machine serving 200 voters in a 14-hour election day serves one voter every 4.2 minutes on average.

In any case, our results are not particularly sensitive to the exact value of v or the proportion of votes cast electronically. For instance, the adversary remains effective even under conservative assumptions where each machine serves 500 voters and 5/6 of votes are cast electronically.[2] Even then, a manipulation of one vote per machine would be enough to overcome the margin for both Florida and New Mexico, and two votes per machine adds Wisconsin and Iowa in the 2000 election.



Electoral college votes changed versus percent popular vote changed.

State	Electoral votes	Vote count			Winning Margin	
		Bush	Gore	Total	Absolute	Percent of total
FL	25	**2,912,790**	2,912,253	5,963,110	537	0.009%
NM	5	286,417	**286,783**	598,605	366	0.061%
WI	11	1,237,279	**1,242,987**	2,598,607	5,708	0.220%
IA	7	624,373	**638,517**	1,315,563	4,144	0.315%
OR	7	713,577	**720,342**	1,533,968	6,765	0.441%

Table 1. Five closest-margin states [3–5].

There were 184,394 voting precincts in the 2000 election [2], for an average of 572 votes cast per precinct. If the adversary is only able to change votes on a per-precinct basis,[3] the outcomes in Florida, New Mexico, and Iowa, and thus the outcome of the election, are still reversed by two vote changes per precinct.

Results

The data given in Table 1 shows statistics for the five closest-margin 2000 presidential election states. These states were all decided by margins of less than half of one percent of votes cast. The figure here shows the number of electoral votes changed versus the percent of the popular vote changed in favor of each candidate. Note that less than a small fraction of one percent of votes needed to be modified to change the winner to Gore, due to the very small margin in Florida, though changing about two percent of popular votes would give either candidate a large margin in the electoral college.

Tables 2 and 3 show the capacity of the adversary to direct the manipulation to the benefit of a particular candidate. In particular, Table 2 indicates that an adversary capable of changing one vote per voting machine could have swung 25 electoral votes from Bush to Gore. This would have made the final electoral college totals 246 votes for Bush versus 291 votes for Gore, rather than the actual 271 votes for Bush versus 266 votes for Gore. Thus, an adversary with the ability to manipulate one vote per machine could have changed the outcome of the 2000 U.S. Presidential election.

m votes manipulated per machine	States swung		
	Count	Electoral votes	Percentage of total electoral votes
1	1	25	4.6%
4	2	29	5.3%
8	5	65	12.1%

Table 2. States swung from Bush to Gore by manipulating *m* votes per machine.

m votes manipulated per machine	States swung		
	Count	Electoral votes	Percentage of total electoral votes
1	4	30	5.6%
4	4	30	5.6%
8	5	40	7.4%

Table 3. States swung from Gore to Bush by manipulating *m* votes per machine.

Conclusion

E-voting machines potentially make electoral fraud unprecedentedly simple. An election saboteur need only introduce a small change in the master copy of the voting software to be effective. As Mercuri noted, "Whereas earlier technologies required that election fraud be perpetrated at one polling place or machine at a time, the proliferation of similarly programmed e-voting systems invites opportunities for large-scale manipulation of elections" [8]. Our analysis demonstrates that even a trivial example of this kind of fraud can be effective.

We have shown that changing just one vote per voting machine is enough to allow an adversary to

[1]Georgia purchased 19,015 [6] voting machines to serve the entire state. If these machines had been used to collect the 2,596,804 votes cast in Georgia in the 2000 Presidential election, then 136 votes would have been cast per machine. Georgia does not have absentee voting. Maryland recently purchased 11,000 [7] machines. In the 2000 Presidential election, there were 2,025,480 [3] votes cast in Maryland. If those 11,000 machines had been used to collect the votes cast in 2000, 186 votes would have been cast per machine. We adopt the more conservative figure of v = 200, providing the adversary fewer opportunities to manipulate the election.
[2]See the recent article in *The Nation* by R. Dugger: www.thenation.com/docprint.mhtml?i=20040816&s=dugger.
[3]Scenarios in which the precinct rather than the machine is the relevant unit of manipulation include manipulating in-precinct optical-scan ballot talliers and realizing some unanticipated efficiency of e-voting technologies that makes only one e-voting machine necessary per precinct.

control the result of this election. Moreover, an adversary able to change a few more votes can swing states with much wider margins, which may be effective in changing the outcome of an election with wider margins overall than those of the 2000 election, or in establishing wider margins for other purposes, such as avoiding recounts and revotes or establishing a mandate beyond merely winning the election.

Such slight manipulations, despite significantly changing the outcome of the election, are small enough that they might plausibly evade detection entirely, be dismissed as random noise if detected, be obscured by noise inherent in the voting and auditing process, or fail to prompt a recount if they are detected but their significance is underestimated or misunderstood.

This emphasizes the importance of a voter-verified audit trail as protection against this sort of pervasive, subtle manipulation. To guard against such an attack, the correspondence between each voter's intentions and the tally reported by the system must be made absolute by such means as the Mercuri method [8], where each voter personally verifies a machine-produced paper ballot that is then counted by machine in a reliable, repeatable manner, but can nonetheless still be counted manually. C

E-VOTING MACHINES POTENTIALLY MAKE ELECTORAL FRAUD UNPRECEDENTEDLY SIMPLE. AN ELECTION SABOTEUR NEED ONLY INTRODUCE A SMALL CHANGE IN THE MASTER COPY OF THE VOTING SOFTWARE TO BE EFFECTIVE.

References

1. Di Franco, A., Petro, A., Vladimirov, V., and Shear, E. *Tiny Systematic Vote Manipulations Can Swing Elections*. Yale University Department of Computer Science, Tech. Rep. YALEU/DCS/TR-1285; ftp.cs.yale.edu/pub/TR/tr1285.pdf.
2. Election Data Services. New study shows 50 million voters will use electronic voting systems, 32 million still with punch cards in 2004 (Feb. 12, 2004); www.electiondataservices.com/EDSInc_VEstudy2004.pdf.
3. Federal Election Commission. *2000 Official Presidential General Election Results*. Updated: December 2001; www.fec.gov/pubrec/2000presgeresults.htm.
4. Federal Election Commission. *2000 General Election Votes Cast for U.S. President, Senate and House*. June 2001, Updated December 2001; www.fec.gov/pubrec/fe2000/gevotes.htm.
5. Federal Election Commission. *2000 Presidential General Election Result*; www.fec.gov/pubrec/fe2000/2000presge.htm.
6. Georgia Secretary of State. *Georgia Counts! Voting Project—Frequently Asked Questions*, 2002; www.georgiacounts.com/faqs.htm.
7. Kohno, T., Stubblefield, A., Rubin, A.D., and Wallach, D.S. Analysis of an electronic voting system. In *Proceedings of the IEEE Symposium on Security and Privacy* (May 2004); avirubin.com/vote.pdf.
8. Mercuri, R. A better ballot box? *IEEE Spectrum 39*, 10 (Oct. 2002); www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html.
9. Miller, H. Electronic voting is solution. *USA Today* (Feb. 4, 2004), 14A.

Anthony Di Franco (anthony.difranco@yale.edu), **Andrew Petro** (microcline@gmail.com), **Emmett** emmett.shear@yale.edu), and **Vladimir Vladimirov** (vladimir.vladimirov@yale.edu) are undergraduates at or recent graduates of Yale University. This article is based on a technical report [1] the authors produced while undergraduates.