

(Note to the reader: This is the original text of the submission. Very minor editing changes were made in the published op ed piece. DAB)

Cindi Scoppe's 8 July editorial says regarding our electronic voting machines (called DREs) that "It's bad enough when a needed cure is worse than the illness. We don't have any evidence to suggest that we're ill."

With all due respect to Ms Scoppe and her sources, it's worth looking at the facts, because the facts seem quite different.

First, we don't have any hard evidence that we are ill because we won't *ever* get any evidence from the current system one way or the other. We are functioning like a bank that accepts deposit slips, with the actual deposits in a sealed envelope, posts the deposits to the ledger, and throws the unopened envelopes into a vault. If the bank never opens the envelopes, it will never have evidence that it has no money. What makes our voting system even worse is that it we actually are *not allowed* to look inside those envelopes because the "vault" is owned by the DRE vendor.

Second, in every study I have seen, of every DRE examined, the computer experts return a vote of no confidence. No study I have seen yields a favorable opinion.

For the ES&S iVotronic (South Carolina's machine), the state of the art analysis is in the EVEREST report submitted in 2007 to the Ohio Secretary of State by teams from the University of Pennsylvania and a California computer security company. Those experts describe the system with three chilling adjectives: "buggy, unstable, and exploitable."

These experts, who have, I suspect unlike the *State* and its sources, actually examined the code and system in great detail, report that the ES&S Unity and iVotronic machines "lack the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions." Vulnerabilities come from

- "ineffective security mechanisms;"
- "incorrect use of security technologies such as cryptography" so that basic security features are neutralized;
- "the visible lack of sound software and security engineering practices" and the pervasive presence of "poor or unsafe coding practices, unclear or undefined security goals, technology misuse, and poor maintenance," leading to "a buggy, unstable, and exploitable system."

Software is hard to get right, and elections are important, and for these reasons the expert recommendation to the federal Election Assistance Commission is that no election system should rely only on software. South Carolina, however, relies only on software, and then places blind faith in software already deemed by the experts who have seen it to be "buggy, unstable, and exploitable." When software with these attributes produces a surprising result, it is perfectly reasonable to suggest that the software is the cause.

The citizens of South Carolina deserve better than buggy, unstable, and exploitable elections. We vote on a complicated computer system (500,000 lines of code, nine programming languages, and four hardware platforms?). It is time to stop listening only to editorial writers and policy wonks and to start paying attention to those who know how to analyze complicated computer systems. That their message is an inconvenient truth is unfortunate, but it is the message we should be listening to.

Duncan A. Buell, 850 Hampton Creek Way, Columbia SC 29209  
803.647.7581 (home)  
803.479.7128 (mobile)  
[buell@ieee.org](mailto:buell@ieee.org)

Dr. Buell is a computer science professor who has provided advice on electronic voting machines since 2004 to the League of Women Voters of South Carolina and who regularly uses the professional analyses of the

iVotronics in class as case studies of How Not to Write Code.