February 22, 2019

The Remote Voting Minefield: from North Carolina to Switzerland

The absentee ballot fraud in North Carolina shows how current vote-by-mail methods are fundamentally flawed and vulnerable to vote-buying and coercion. But banning remote voting of any kind would disenfranchise everyone not living in their country of citizenship; that is not a real option.

It is important to understand in this light the context of the Swiss e-voting project, one of whose two implementations was recently opened to public inspection by the Swiss Post for inspection and analysis by international experts. Almost everyone in Switzerland votes by mail. Despite its well-known vulnerability to fraud, coercion, or vote-buying of exactly the kind we see in North Carolina, Switzerland adopted postal voting from 1978 to 2006 for voter convenience and engagement.

Due to its tradition of direct democracy, Switzerland asks citizens to vote four times per year, not just once in 2-4 years as in the US. If you're asking people to read up on and vote on dozens of issues several times a year, it had better be convenient.

Then there's the expat issue. Swiss citizens living abroad, even in neighboring European countries, don't get voting rights there like moving to another state in the US. About 11% for Swiss citizens live abroad, in contrast to more like 3% of US citizens. Switzerland's population is similar to New York City's. If Switzerland disallowed remote voting, it would be like NYC disenfranchising any New Yorker who moves elsewhere until they spend 10 years establishing new citizenship in Jersey or Upstate New York.

Taking a position of "no remote voting" in a small country like Switzerland would be not just unrealistic but flat-out undemocratic. Given this reality, the Swiss voting authorities have the challenging and unenviable task of navigating a minefield of imperfect alternatives.

At regulation and design level, the Swiss E-voting project is the most technically solid I've seen anywhere, mandating end-to-end encryption and universal verifiability all the way from vote entry through shuffling and counting in the split-trust back-end. Another important distinction of Switzerland's approach is its requirement that "the source code for the system software must be made public" - a huge advance over the standard practice of governments almost anywhere else in the world.

No system meeting these requirements can realistically be expected to be simple. Now that the source code for one of the two independent implementations has been published, it's no surprise that experts are finding issues and worrying about its complexity. But that is the whole point of the carefully-regulated, open approach Switzerland is taking: to find flaws, fix them, iteratively improve design and implementation practices, and deploy E-voting cautiously and gradually among limited populations in participating cantons.

Those who oppose any E-voting due to its complexity fail to consider how alternative methods of remote voting may be even worse. Postal voting puts the entire complex and opaque postal mail system, with all its workers and automated mail-handling systems, on the trusted path. Properly-designed E-voting can enable voters to verify independently that their vote was correctly conveyed to the voting authority and not lost (or "lost" by a miscreant) and that it was shuffled and tallied correctly, without trusting any single human or electronic device. The "average voter" certainly won't understand all the code and cryptography in an E-voting system. But if the source code is open to public inspection, any voter can find or hire an expert of their choice to analyze it. Will your postal service let you send your choice of expert to inspect their operation?

International scrutiny of E-voting systems like Switzerland's is extremely important and welcome. But simplistically opposing all E-voting, on grounds of complexity or failure to solve problems like vote-buying that alternatives like postal voting have too, is counterproductive. The only way to solve critical open security challenges like vote-buying is to press forward and work to advance the state-of-the-art further, not retreat to a techno-luddist position that any voting method using paper is automatically more secure than any method using electrons.

Estonia's approach of allowing "re-voting", where a voter who cast a vote under coercion can later replace it with different vote when no longer under coercion, has its flaws but is pointing in the right direction. The idea of "decoy ballots" in Chaum's recent proposal of Random Sample Voting and its derivative Alethea is also an important and interesting idea that's definitely pointing in the right direction, if not yet a perfect solution either.

Highly-mobile citizens of modern democracies need the ability to vote conveniently, from outside their home town or country when necessary. Just saying that no remote voting technology is safe may be simplistically true but is unhelpful. No voting technology is perfectly safe. We can prevent future disasters like North Carolina only facing forward, not back. A technically-informed, systematically-designed, cautiously-deployed, open approach like Switzerland's E-voting project is what tech security people need to embrace and improve, not dogpile.

Note: this blog post is a reformatted and lightly-edited version of this tweet thread.

Updated 8-Mar-2019 to reflect that the Swiss Post code is open to public inspection but not "open source" by standard definitions.

Disclosure: my DEDIS lab at EPFL was recently involved in funded research collaboration with one of the two Swiss E-voting implementation projects (CHVote from Geneva, not the Swiss Post project mentioned above). I am not otherwise affiliated with either project. The views in this post are solely my own.

Bryan Ford