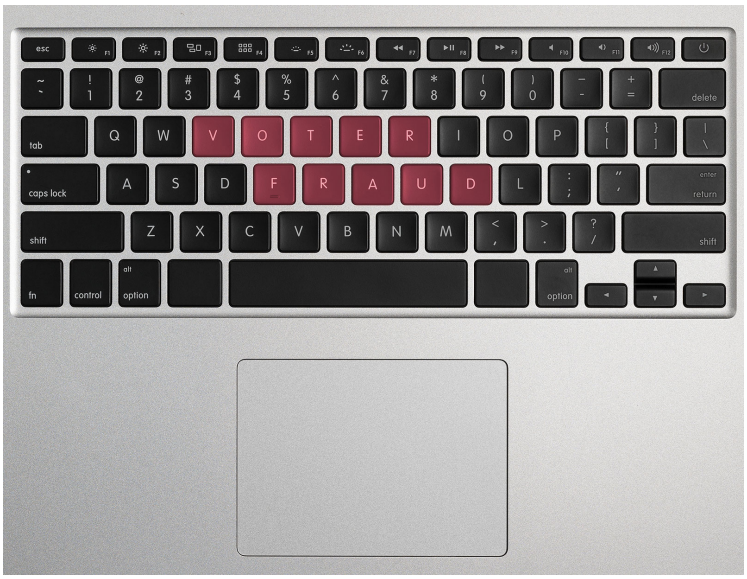
SAN FRANCISCO SINCE 1865
Examiner

Tuesday February 14, 2017

Open-source voting is the answer to hacking concerns



Unlike proprietary voting systems developed by corporations, open-source voting is public, transparent and allows for the highest level of scrutiny. (Courtesy photo)

By Maureen Erwin on January 19, 2017 1:00 am

Will we ever have a voting system that is completely error-proof and impenetrable from malicious forces? Not likely. But the security breaches that are increasingly a part of daily life serve as a call to action.

Every day brings a new report of hacking or suspicious activity, and increasingly with fingers pointing to international actors. Whether it is statewide voter registration databases (Illinois and Arizona; some say more); national party organizations (the Democratic National Committee); utilities (Vermont's Burlington Electric); or Russia's state-run television station (RT) suddenly interrupting C-SPAN last week — the incident is still under investigation and not confirmed as a hack — it is all very unsettling and leaves us feeling vulnerable.

Knowing that suspicious events are investigated and steps are taken to make our systems more resilient brings us some small sense of reassurance that at least someone is looking at it, and something is being done. But what about our voting systems? We must have some level of basic confidence that our elected leaders — whether we personally support them or not — got there with a system we have confidence in.

↓ **Continue Reading Below**

Trending Articles

Chinese New Year Parade lights up downtown SF

Supervisors blast Muni for not using bond money that was, in turn, blocked by supervisors

Wiener proposes major fundraising legislation for transportation agencies statewide

BART directors introduce 'sanctuary in transit' policy to protect immigrants

Chinese New Year Parade sees passing of torch

Have we reached a post-truth era?

Nationally, our voting machines are generally a patchwork of proprietary systems that ostensibly meet certain standards for functionality and security by federal and state bodies. Some systems produce paper ballots that can be used to audit results; some are all-electronic, meaning voter intent is registered and tabulated through a system of memory cards and machines.

It is important to note that, so far, no one has revealed any convincing evidence that any of our nation's voting machines produced results due to a hack in November. We can't prove it happened, but how sure can we be sure that it didn't happen?

Are there logs that would leave footprints if systems were breached? Could a hacker insert code that wipes the log as the last step of the breach? We don't know because the systems are proprietary. They are the intellectual property of the corporations that develop them, which basically means it's none of our business.

The fact that voting machines run on proprietary software and use as many as hundreds of thousands of lines of code to function means only a very small group of people are in any position to vouch for their security. The rest of us must trust them. Many elections officials across the country continue to assure us that all is safe. Their job is to create confidence in the system. But if a system isn't secure and needs to be fixed, who do these assurances serve? It's like saying as long as we assure everyone the house isn't on fire, nothing is burning.

History doesn't look kindly on people who kept everyone calm and comfortable while their house burned down around them. It rewards the people who called the fire department before it was too late.

Most election officials are not technical experts, and the code isn't available for them to examine anyway. And do we really expect local or state IT departments, which may be up to keeping their systems running and safe from most threats, to be a match for masters of cyber espionage?

be constantly examined for functionality issues and vulnerabilities? That is what the proponents of open-source voting advocate for. If all goes as planned, San Francisco is set to implement open-source voting for our local elections, as soon as 2019.

Unlike proprietary voting systems developed by corporations, which are not available for broad scrutiny and require placing a lot of trust in a small group of people, open-source voting is public, transparent and allows for the highest level of scrutiny. Advocates point to long-term cost savings as well.

If we can't make a perfect voting system, we could have a vastly improved system with an open-source system that utilizes a mandatory paper ballot of record that can be easily recounted and audited. We might be wise to follow the guidance of a Russian proverb: Doveryai, no proveryai, which translates to "trust, but verify." San Francisco can help lead the way.

Maureen Erwin is a Bay Area political consultant. Most recently she led Sonoma County's Measure M, which will create the largest GMO-free growing zone in the U.S.