Written by **C. Mitchell Shaw** on August 31, 2016

Hacking Elections: How Easy Is It?

As if the issues of an ill-informed electorate, media smear campaigns, and partisan politics weren't enough to make elections difficult affairs, there is a not-so-new twist in the plot that will — at the very least — undermine many informed voters' confidence in the system. Enter — from somewhere hidden offstage — the hackers who may well have more control over the outcome of November that any voting bloc could hope for.

Technology is a wonderful servant. It is also a terrible master. As people have become more dependent on technological tools that didn't even exist a decade ago, they seem to sort of fade into the background. Until they fail or betray their users. Think about it: How many phone numbers do you actually *know* any more. There was a time when everyone knew the numbers of the places they call on a regular (or even semi-regular) basis. Now, your phone remembers those for you. You just pull up the name and touch an icon. The phone does the rest. Until you are out somewhere and your battery dies, or you drop and break your phone. Then you realize that you have given control over what you know to a device. And it has failed you.

There was a time (not too long ago) when voting was done on paper ballots. Those ballots were counted and the results were announced. If there was a dispute, the ballots were recounted. The process was slow, and in a world where people expect to know results almost immediately, slow was considered bad. Now, it's all done by computers. In some places the computers count paper ballots. More often that not, though, there is no paper involved. The voter touches an icon or presses a button and registers his vote. But what if the voting machine — which is, after all, just a computer — has been compromised by any of a number of methods? What if the machine is set to register your vote for "candidate A" regardless of which icon you touch or which button you press? That is not as Hollywood as it may sound.

After all, Andrés Sepúlveda — who is serving a 10-year prison sentence for "charges including use of malicious software, conspiracy to commit crime, violation of personal data, and espionage, related to hacking during Colombia's 2014 presidential election" — made a good living hacking elections all across Latin America before he got caught. According to a report by *Bloomberg Businessweek*, Sepúlveda hacked nearly everything related to elections that ran on computer code. And while most votes in the nations where Sepúlveda was busily plying his skills do not rely on voting machines the way we do here, it is no big leap from what he did to hacking voting machines.

In fact, back in 2007, Princeton professor Andrew Appel demonstrated just how easy it is to replace the firmware of a "trusted" voting machine to hack the results of an election. He purchased a used voting machine online, opened it with the provided key (other keys are available online, as well), removed 10 screws to expose the innards of the machine, and hacked it to show one vote on the screen and another vote in the count. In other words, the voter would see his choice confirmed on the monitor, but his vote would be counted for another candidate. As Appel wrote:

> If I had the inclination to cheat in an election (which I do not) I could prepare a modified version of

the firmware that subtly alters votes as the votes are cast, with no indication of the alteration made visible to the voter. I would write this modified firmware onto new ROM chips. Then, if I had access to one of New Jersey's voting machines (for example, in an elementary school or firehouse where it is left unattended the night before an election), I could open the door of the machine, unscrew 10 screws, replace the legitimate ROM chips with my own fraudulent ones, reinstall the cover panel with its 10 screws, and close the door of the machine.

Even without the key, opening the machine is child's play. "Although I used a key to open the lock, the lock itself is a fairly simple one, Appel wrote, adding, "I watched a Princeton University student pick the lock of my machine in about 7 seconds."

Given that many voting machines are connected to a network to allow them to send the results of their data to a central location to be tallied *in toto*, hacking the firmware would not necessarily require physical access to the machine. It is not a wonder that it could be done; instead it is a wonder it hasn't *already* been done. But then, it could have been done, and who would know? The implications are staggering.

With the recent hack of the Democratic National Committee's e-mail servers and data systems, the powers that be are suddenly concerned about a problem techno-nerds have been trying to draw attention to for years. Given, election results are slow when paper ballots have to be counted, but really, when the people of a state or nation are electing the politicians who are going to write and execute the laws that will touch the lives of those people, which is more important, immediate results or security?

In the end summation, voting machines need to go away. At the very least their purpose should be restricted to counting paper ballots which are then recounted by hand for accuracy. And every single one of those machines should run on open-source software that can easily be audited for vulnerabilities, which can then be patched quickly. After all, if a voter is not intelligent enough to color in a circle or a square on a paper ballot, should they even be voting for a congressman, president, or senator that the American people are going to have to live with for two, four, or six years? Hanging chads and all, that system beats a hacked system hands down.

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.

What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.

Subscribe