Written by **Joe Wolverton, II, J.D.** on October 11, 2011

Electronic Voting Machines Proven Vulnerable to Hacking

If the above is accepted as true, then the perpetuation of the American Republic is in peril.

To understand the scope of the threat to U.S. elections, one must keep the following fact in mind: Almost all voters in Georgia, Maryland, Utah, and Nevada, and the majority of voters in New Jersey, Pennsylvania, Indiana, and Texas, will cast their ballots using electronic voting devices on Election Day in 2012.

Now follows the chilling report published in *Salon*: "Voting machines used by as many as a quarter of American voters heading to the polls in 2012 can be hacked with just $10.50 in parts and an 8th grade science education."

This is the fragile state of affairs according to the computer science and security experts employed at the Vulnerability Assessment Team at Argonne National Laboratory in Illinois. After conducting numerous experiments on the machines used by millions of American voters, this group of experts reportedly found that “the newly developed hack could change voting results while leaving absolutely no trace of the manipulation behind.”

The head of this cadre of computer consultants, Roger Johnston, warned:

> We believe these man-in-the-middle attacks are potentially possible on a wide variety of electronic voting machines. We think we can do similar things on pretty much every electronic voting machine.

The sample machine used by the Argonne team was the Diebold Accuvote voting system. The device was obtained from a “former Diebold contractor.”

While previous laboratory experiments on the vulnerability of similar devices demonstrated that an extraordinary amount of coding savvy would be required to hack these electronic voting machines, this latest investigation showed that for an attack on the machine’s software to be successful, “no modification, reprogramming, or even knowledge, of the voting machine’s proprietary source code” was necessary.

A video of the experiment is available at bradblog.com.

It isn’t as if the Argonne findings are novel. In fact, for years scientists — of both the political and computer variety — have sounded alarms regarding the security of these machines that are playing an increasingly key role in numerous elections around the country. According to the *Salon* piece, many experts inside and outside of the government have declared repeatedly that improvements in technology and the ready availability thereof were making tampering with these devices not only simple, but likely irresistible.

Admittedly, the placement of the type of machine used in the Argonne experiment — the touch-screen Direct Recording Electronic (DRE) voting systems — has decreased slightly as news of its vulnerability has spread. However, a DRE machine nearly identical to the one hacked for 10 bucks by members of the Argonne team will be used again in November 2012. Deployment by states of these easily manipulated machines is astounding in light of experiments and findings thereof reported for years now.

The most alarming aspect of the widespread reliance on these DRE machines is the fact that according to verifiedvoting.org, nearly one-third of Americans who will cast votes on Election Day 2012 will have no choice but to do so using one of these devices. Citizens of states exclusively employing the voting machines should immediately recur to their state government for an explanation of such a seemingly inexplicable decision.

Equally disturbing is the specter of nearly every voter in Georgia, Maryland, Utah, and Nevada, and the majority of voters in New Jersey, Pennsylvania, Indiana and Texas, touching the screen, trusting that their vote will be accurately recorded and tabulated. Incredibly, voters in some of America's largest cities will find these machines waiting for them inside the voting booth next year for use in state and municipal elections.

Houston, Atlanta, Chicago, and Pittsburgh are just a few of the metropolises scheduled to roll out this "technology" before next year. Every one of the machines ordered by these cities is of the same variety hacked so effortlessly by workers at the Argonne National Lab.

Hackers are the bane of the manufacturers of these voting machines. For decades, developers, designers, and programmers have worked with genuine determination to create a machine impervious to those who would attempt to alter or abolish votes cast on these devices. The problem is that most of these protective measures are aimed at those outside the system trying to break in. The immediate concern now, however, comes from the potential for abuse by those insiders who have unfettered and unregulated access to the machines and the software that runs on them.

"This is a fundamentally very powerful attack and we believe that voting officials should become aware of this and stop focusing strictly on cyber [attacks]," says Vulnerability Assessment Team member John Warner. "There's a very large physical protection component of the voting machine that needs to be addressed."

The extent of the threat from those with malevolent design is demonstrated by the video produced by the Argonne team. In the video a hacker inserts a small electronic device into the machine that gives him remote control capability from up to half a mile away.

"The cost of the attack that you're going to see was $10.50 in retail quantities," explains Warner in the video. "If you want to use the RF [radio frequency] remote control to stop and start the attacks, that's another $15. So the total cost would be $26."

How and when would such manipulation take place? Argonne Team leader Johnson explains that the tampering would happen after votes have been cast by citizens believing the system to be safe and believing that their vote has been counted. Johnson says that the type of attack demonstrated in the video would likely happen on or around Election Day after the machine has served its electoral purpose. He also indicates that the alterations to the guts of the machines could be done during "sleepovers," the nights prior to Election Day when the devices are kept at the homes of poll workers for safekeeping.

Frighteningly, the Argonne team found that the inspection measures currently in place are woefully

inadequate. According to members of the team, such inspections rarely include physical inspection of the inner workings of the device. Even if such reviews were made, the team posits that when carried out by someone who knows what he's doing, the hack leaves behind little or no detectable trace.

"The really nice thing about this attack, the man-in-the-middle, is that there's no soldering or destruction of the circuit board of any kind," Warner says. "You can remove this attack and leave no forensic evidence that we've been there."

How does the hacker committed to affecting the free elections of the United States gain access to the insides of the machine? Apparently, the lock is easily picked and alternatively, the key to the lock is easily copied and is a common variety used in many low-security commercial locks.

The picture is clear: With $30 in his pocket, a person could make a trip to Radio Shack and remotely access and alter votes cast in good faith by citizens counting on the reliability of our electoral system.

Photo: AP Images