

# Can a Voting Machine that is Rigged for a Particular Candidate Pass Certification?

Avi Rubin  
Johns Hopkins University

The computer security community claims that today's fully electronic paperless Direct Recording Electronic (DRE) voting machines are insecure. The vendors and some in the elections community maintain that they are perfectly secure and that the procedures that are used can overcome any security problem. The Election Assistance Commission, the rest of the elections community, and the public are left wondering whom to believe.

My greatest concern with paperless DREs is that whoever makes the machines has the capacity to rig election results however they like. Proponents of DREs argue that the ITA process would catch any attempts to manipulate the results. They argue that Trojan horse programs would have to have magical properties and that they would be detected. They further argue that techniques such as parallel testing, where machines are selected at random and elections are run on them on election day where they are checked for accuracy, ensure that no such rigging is possible. Security experts do not buy these arguments.

I propose a challenge.

This is not a hacking challenge where a team of computer security experts tries to break into a system or tamper with voting machines. That is not my primary concern with voting equipment. My challenge is aimed directly at the certification and deployment process for DREs. The purpose of my challenge is to test whether or not a machine that is deliberately built to favor one candidate in a federal election could make it through existing processes and into actual voting booths. (Of course, the rigged machines would not actually be used.) To explain my idea, let me draw an analogy. US airports take security very seriously. They deploy a multitude of security guards, X-ray machines, dogs, and sophisticated chemical detection equipment. From time to time, they send undercover agents with real weapons to try to sneak them through the system and get on an airplane. These tests accomplish two very important things. First, they are capable of discovering security weaknesses. Second, the security guards are aware of the potential for these tests, and so they are more vigilant. Implementing my challenge would have the same two effects on the security of voting technology.

Here is what I propose. I form a team of computer security experts. We produce a DRE voting machine that is rigged to favor some candidate in a national election. Obviously, we do not have the resources to produce a fully functional system in software and hardware – it takes companies millions of dollars of investment and multiple years. Thus, I propose that my team be given access, under full non-disclosure, to the development environment, hardware and software, of one or more of the four major vendors of DREs. We then modify these systems as we see fit to produce a rigged voting machine. Next, several states are chosen at random, and our rigged machine is submitted to the ITA for certification exactly as though it were being submitted by the original vendor. Nobody at the state or ITA level will know that they are part of a security test, as opposed to certifying a real system. The challenge would be to see if the rigged machines successfully make it through the process.

What would such a challenge teach us? Like all security challenges, it will only produce a definitive result if there is a security problem. If the rigged machine does not make it through the process, while we will not be able to conclude that the system is secure (just like successfully catching an agent with a concealed weapon at the airport does not mean that the next guy won't get through), we will have more confidence in the process than we have today. On the other hand, if all of the rigged machines get certified in all of the chosen states, then we know that the vendors could just as easily rig the election.

Practical considerations:

1. To successfully manage this challenge would require the full participation of election officials to require the vendors to submit their systems under non-disclosure to my team. The Election Assistance Commission could play a role in this, and if they decided to embrace this idea, is probably in the best position to make this work.
2. It would be useful to have a budget to compensate my team for their time and some travel for face to face meetings, although my participation would be pro-bono. Without funding, I would still try this, but it would be more challenging to get busy people to volunteer their time and energy. If the EAC gets funded properly, perhaps they could subsidize this effort.
3. It is critical that the ITAs have no idea whether they are receiving the real system from the vendors or our rigged system. Since the ITAs are currently in the employ of the vendors (something that is severely broken), this would present some difficulty, but with the cooperation of the vendors, forced or voluntary, it could be made to work.
4. While this challenge may teach us a lot, it should be noted that a vendor wishing to rig an election could be funded by a multi-billion dollar entity. Their ability to rig the election when building a system from scratch is much higher than that of my team, attempting to bury the fix inside an existing system. Furthermore, familiarity of the existing system by the ITAs could highlight the changes made by my team. If the real vendors were to work with the ITAs to try to find our rigged system, they could use software tools to find the differences between the existing system and the one we provide. That said, if the states given the rigged system are chosen at random, I have high confidence in our ability to get a rigged machine passed.
5. If the rigged machine makes it through the entire process and is certified in every state where it is tested, and if we are able to show that indeed the machines would have produced a fixed result, regardless of how people vote, then we need to move to permanently eliminate such voting equipment from our elections.
6. The very fact that I have proposed this challenge will hopefully cause greater diligence by the testers, who from now on do not know if an agent is trying to sneak a loaded gun through security or not.