

## **Hacker's public testimony at Cuyahoga Board of Elections forum on Diebold voting machines**

The following is the public testimony submitted by a cleveland-area hacker at the October 17th Cuyahoga County Board of Elections' public hearing on the Diebold AccuVote (tm) touch-screen voting machines. It contains a summary of the 300 pages produced by Compuware, the company hired in Ohio to audit the Diebold AccuVote machines, plus additions by the hacker.

###

Hello.

I am a professional hacker who has been living in Cleveland for the past seven years. Due to misconceptions I feel I should explain that term, Hacker. We are all familiar with the negative connotation of Hacker, namely a person who exploits flaws in computer systems for amusement or for personal gain. We've seen these people in the news getting arrested for stealing credit card information or social security numbers, and the news media sometimes calls them Hackers. Well, they are not hackers. In the computer security field, a hacker is someone that is intimately familiar with the hardware and software that make up various computer systems, so familiar in fact that we can find unknown flaws in those systems and fix them. When I say I am a professional hacker, that means I am paid regularly by companies to develop hardware and software packages that are secure from unwanted intruders. It's a great job, I don't even have to wear a suit, and people still invite me to their business lunches.

On a weekly basis I read about 200 emails on various computer security mailing lists. I am not an academic, I am fully engaged in writing and auditing secure software. I can tell you how to hack into your own computer. I can tell you some surprising things. Here at this public hearing, there are at least two people in this room using bluetooth cell-phones that need to be updated because they are hackable. If someone really wanted to they could listen in on your conversations, steal your saved phone numbers, and rack up huge bills on your cell phone. There's a public wireless internet connection available in this room, and for everyone that turned on their laptop over the break, did you know that your wireless card might be connecting to the public wireless network without asking? Did you know that your email program is still trying to check your email? Did you know that your username and password could have been swiped by anyone here with a laptop?

I have been following the progress of touch-screen voting since the 2000 election cycle. Having written software professionally for the past decade, I understand the attraction to touch-screen voting. The machines could be easy to use, to the point where we would reasonably expect most voters to vote without error. That would be an amazing improvement on our current punch-card system. The machines can display instructions in different languages, and even allow the blind and others with unique voting needs to vote without assistance. That's amazing, that represents true progress both in technology and in democracy. The downside of course is that computer systems are hackable. The same kind of flaws that freeze up your PC at home are the same kind of

flaws that allowed criminals to steal over 40 million credit card numbers from a computer system in June of this year, and it's these same kind of flaws that are going to allow people to change votes with the Diebold AccuVote system. I am here to talk about those flaws. For the Diebold personnel in the audience, I understand your position. I know what it feels like to have a system I've written or chosen criticized, it hurts my feelings and it feels like people are attacking me. At the same time I know somewhere in the back of my mind that it's necessary for people to do this. Even when it makes me defensive or uncomfortable, I know that I want my software to be safe and I know that people might find ways into my systems that I never dreamed of. So I listen, and I hope you will too.

The Diebold AccuVote system was audited back in 2003 by Compuware, which is a computer security firm out of Columbus, at the request of the Ohio Secretary of State. I read all 244 pages of the audit, which detailed the security flaws in three other voting systems besides the Diebold system. At that time, the security on the Diebold system was such that almost anyone could tamper with the election results. Voters could lockup the machine by pressing F4 on the keyboard and trying to re-run the election software. Poll-workers could use the supervisor card, with a factory-set password of 1111, to close the polls early or reset the counts at any time. Election officials had it even easier, if you were anywhere near the Tallying computer all you needed to do was open up the results file with Microsoft Access and change the vote tallies. You could even do it over the network! After Diebold had almost a year to fix the problems, the next Compuware audit in August of 2004 still found major problems with the AccuVote touch-screen voting system. Although Diebold added some encryption to their system and removed the keyboard port, the audit still showed that all you needed to modify election results was a copy of Microsoft Access. Finally in January of 2005 a third assessment by Compuware showed that most of the issues they had raised with Diebold's software had been resolved. That's where I want to jump into the discussion. Compuware did a professional job of raising obvious security concerns and following through on them with Diebold.

Did you notice that the voting machines have audio versions of the election in them, so that people with vision trouble can vote unassisted? Did you know that the audio for this, the parts that tell you which candidate you're supposedly voting for, these audio clips are stored unencrypted on a simple PCMCIA hard drive, the kind that you plug right into your laptop or palm pilot? All you have to do to mess with the election results is bring a small flathead screwdriver, pop open the cheap plastic panel, grab the PCMCIA card, plug it into your palm pilot, and switch the audio clips so you think you're voting for your candidate but your vote is actually given to someone else, and you'll have no way of knowing it. Although the expensive Compuware audit recommended these be encrypted, they are still left unencrypted and ready for fun. There is a security provision on these, there's what's called a security signature on the files, and this signature is stored elsewhere in the voting machine. If the files are altered, the signature will change, and the voting machine should detect the problem. However, Diebold chose a signature algorithm called CRC, which is very easy to hack. You just need to make tiny changes in the modified audio until the signatures match, and once again your election fixes go unnoticed.

More dangerous though, is the potential for people to modify their voting cards. With the Diebold system, voters are given credit-card sized devices called smart-cards, which activate the voting machine. When you are done voting, the voting machine deactivates the smart-card, which is supposed to prevent people from voting multiple times. A lot of people think that smart cards are the equivalent of computer security, just like a deadbolt lock is a good amount of physical security. This is only true however, if your machine uses all the encryption features of a smart-card. Smart-cards can provide a nearly unhackable authentication, but the Diebold AccuVote doesn't use that feature. Because of this, it is possible to use what's called a "replay" technique to reverse-engineer the protocol that Diebold uses. Then you can program your own cards, and bring them into the voting machine with you to cast as many votes as you'd like. With a hand-held smart-card programmer, you can even upgrade your smartcard to a supervisor card or an administrator card. Once you've done that, you can restart polls, close the polls early, or even put the machine into demo mode so it looks like everything is working as usual until you try to tally the votes and find that none of the votes got recorded. In 2003 a copy of the Diebold AccuVote software source code was leaked onto the internet. With this source code you can see how the smart-cards are used, and use that as a starting point for altering the elections.

But that's hard! That's not something that a typical computer technician can do. On one hand that means people are going to dismiss the huge potential for trouble with this. They'll say it's too hard and nobody is going to be able to do it without being noticed. For the dedicated hacker however, it will be possible to cast multiple votes in the 2006 election cycle. On the other hand though, it means that people are going to look for easier ways to alter the system. What I would do if I was really interested in tilting the election towards my candidate, is purchase a set of rare earth magnets from our local electronic surplus store. In Cleveland there's one on 55th and Broadway, that's not too far from here. I would give these rare earth magnets to friends going into polling places where my candidate is likely to lose by a large amount. My friends would simply rub the magnets along the top left of the voting machine, where the removable storage device is, and also the rear middle of the voting machine, where the flash memory is. This would ruin the poll results and destroy the machines in that polling location. By the time the poll workers went through the normal system checks, tried to call tech support, and eventually tried to reprogram the machines, voting would be over and many voters in opposition territory would have been able to vote.

The biggest flaw I've seen in this system though, is the Vote Tallying computer that Diebold plans on installing at the Board of Elections. The database that holds the entire county's votes is stored in Microsoft Access, with no password and no encryption. It's possible for anyone with an IT degree to change voting results at the board of elections. An intern could walk in while nobody's looking and tilt the election of the entire county. Recently Diebold added a small amount of security to try to prevent this. They put a piece of software called Digital Guardian on the server, which monitors and protects alterations to the database. The way around this is so simple it's laughable. You can either start Windows in Safe Mode, so that Digital Guardian doesn't start, or you can

boot the computer from a floppy and then go on to make your changes to the database of votes.

People will say, we can't avoid voter fraud. If someone wants to rob a bank, they're going to rob a bank. The thing is if you owned a bank, you'd want to at least know if your bank has been robbed. In 2006 hackers will be able to change election results and you won't even know it. You'll end up calling it a successful election.

###