



<a href="#">Mission</a>
<a href="#">The Problem</a>
<a href="#">In the News</a>
<a href="#">About Open voting</a>
<a href="#">About Us</a>
<a href="#">Contact Us</a>
<a href="#">Donate</a>

**OPEN VOTING FOUNDATION**

9560 Windrose Lane  
Granite Bay, CA 95746  
Phone (916) 295-0415  
alan@openvoting.org

PRESS RELEASE -- JULY 31, 2006

FOR IMMEDIATE RELEASE

Subject: WORST EVER SECURITY FLAW FOUND IN DIEBOLD TS VOTING MACHINE

Contact: Alan Dechert

Reference: [PICTURES](#)

(Click on thumbnail. Click again on lower half of picture for high resolution)

SACRAMENTO, CALIFORNIA -- "This may be the worst security flaw we have seen in touch screen voting machines," says Open Voting Foundation president, Alan Dechert. Upon examining the inner workings of one of the most popular paperless touch screen voting machines used in public elections in the United States, it has been determined that with the flip of a single switch inside, the machine can behave in a completely different manner compared to the tested and certified version.

"Diebold has made the testing and certification process practically irrelevant," according to Dechert. "If you have access to these machines and you want to rig an election, anything is possible with the Diebold TS -- and it could be done without leaving a trace. All you need is a screwdriver." This model does not produce a voter verified paper trail so there is no way to check if the voter's choices are accurately reflected in the tabulation.

Open Voting Foundation is releasing 22 high-resolution close up pictures of the system. [This picture](#), in particular, shows a "BOOT AREA CONFIGURATION" chart painted on the system board.

The most serious issue is the ability to choose between "EPROM" and "FLASH" boot configurations. Both of these memory sources are present. All of the switches in question (JP2, JP3, JP8, SW2 and SW4) are physically present on the board. It is clear that this system can ship with live boot profiles in two locations, and switching back and forth could change literally everything regarding how the machine works and counts votes. This could be done before or after the so-called "Logic And Accuracy Tests".

A third possible profile could be field-added in minutes and selected in the "external flash" memory location, the interface for which is present on the motherboard.

This is not a minor variation from the previously documented attack point on the newer Diebold TSx. To its credit, the TSx can only contain one boot profile at a time. Diebold has ensured that it is extremely difficult to confirm what code is in a TSx (or TS) at any one time but it

is at least theoretically possible to do so. But in the TS, a completely legal and certified set of files can be instantly overridden and illegal uncertified code be made dominant in the system, and then this situation can be reversed leaving the legal code dominant again in a matter of minutes.

“These findings underscore the need for open testing and certification. There is no way such a security vulnerability should be allowed. These systems should be recalled”

OPEN VOTING FOUNDATION is a nonprofit non stock California corporation dedicated to demonstrating the need for and benefits of voting technology that can be publicly scrutinized.

###

### **Mission**

The primary objectives and purposes of this organization shall be: to educate the public and governmental officials and entities concerning elections systems based upon open source software, and further to promote the adoption of open source voting and elections solutions worldwide.

We believe that vote tabulation must be publicly observable, and that proprietary hidden software code makes public observation of tabulation impossible

Open Voting Foundation is a nonprofit nonstock corporation applying for tax exempt status as a 501(c)(3) organization.

Help us make this a reality. Help us help you.

[DONATE NOW](#)