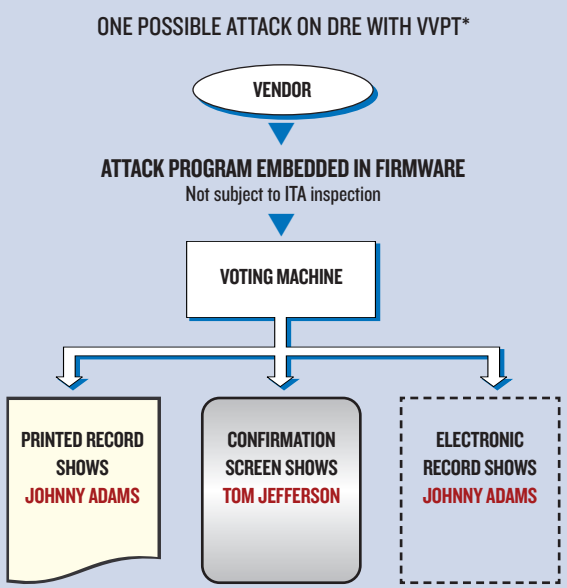
The potential vulnerabilities in an electronic voting machine



*DRE = Direct Recording Electronic voting machine
VVPT = Voter Verified Paper Trail

The Brennan Center at New York University Law School's technical analysis of electronic voting found 120 possible ways of hacking into electronic voting systems. These hacks would work on a direct-recording electronic voting system using a voter-verified paper trail, the report said. Three windows of opportunity for hacking a system appear below.

BEFORE PURCHASE, the system would be vulnerable at the following points of entry not checked by an independent testing authority:

- Interface between the voting machine and the vendor's firmware or hardware
- Interface with the machine's commercial software
- Interface between the machine and the commercial operating system.

AFTER A VOTING MACHINE HAS BEEN PURCHASED, there are three potential points of vulnerability:

- linterface between input and output devices and the voting machine
- Interface between the machine and ballot definition files
- Interface between commercial software updates and patches, and the voting machine.

ON ELECTION DAY, the units are subject to the following vulnerability:

- A hacker could activate a "cryptic knock" sent to the voting machine. A cryptic knock is a user action that triggers or silences an attack. Various means could prompt the knock, such as voting for a write-in candidate, tapping a specific spot on the machine's screen or accessing the unit via a wireless network.