KEY POINTS

Department of Energy took apart Diebold and Sequoia voting machines to show vulnerabilities

$26 in parts and eighth-grade science were sufficient to manipulate election outcomes

Electronic voting declared a "national security issue"

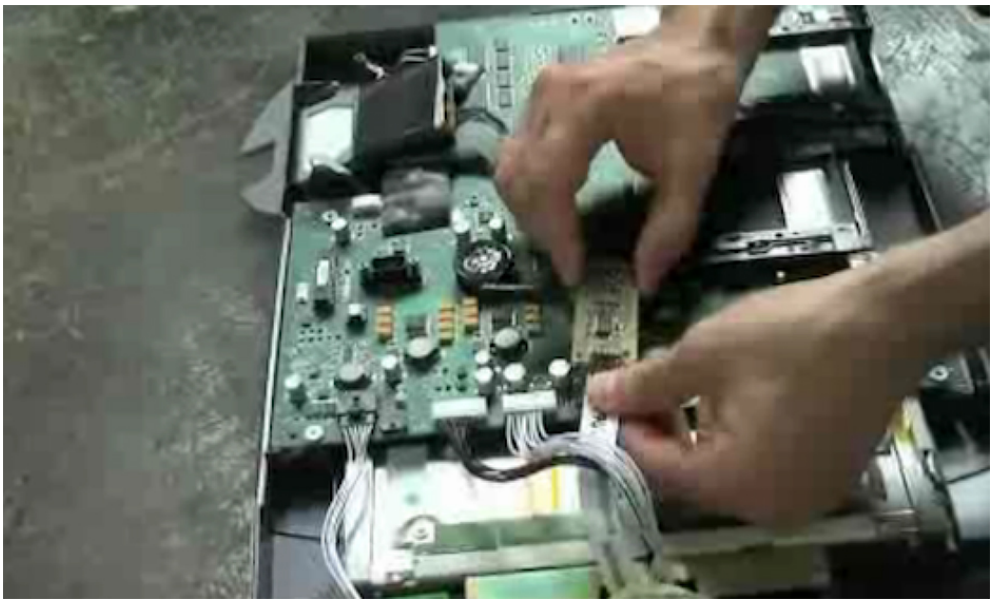
Millions of voters used insecure voting machines in 2012

11 states used voting machines without a paper audit trail

Diebold and Sequoia never responded to the DOE findings

PART FIVE

NATIONAL LABORATORY DEMONSTRATES HOW EASY IT IS TO HACK ELECTRONIC VOTING MACHINES



Researchers on the Vulnerability Assessment Team took apart voting machines to demonstrate how easy it would be to rig elections with only minimal scientific knowledge and very cheap materials. PHOTO: Argonne National Laboratory (PD).

As recently as September 2011, a team at the U.S. Department of Energy's Argonne National Laboratory hacked into one of Diebold's old Accuvote touchscreen systems. Their report asserted that anyone with $26 in parts and an eighth-grade science education would be able to manipulate the outcome of an election.

"This is a national security issue," wrote the Argonne team leader, Roger Johnston, using the sort of language that would normally set off alarm bells in our security-obsessed culture. Yet his warning has gone unheeded, and the Accuvote-TSX, now manufactured by ES&S, will be used in twenty states by more than 26 million voters in the 2012 general election.

Johnston's group also breached a system made by another industry giant, Sequoia, using the same "man in the middle" hack—a tiny wireless component that is inserted between the display screen and the main circuit board—which requires no knowledge of the actual voting software. The Sequoia machine will be used in four states by nearly 9 million voters in 2012.

> This is a national security issue. The manufacturers seem to be in denial on some of these issues.
>
> — Roger Johnston

Why did a physicist choose to hack into voting machines? “This was basically a weekend project,” Johnston told me, expressing his amazement at the meager funding available to examine America’s voting systems:

> *We did it because a lot of people looking at the machines are cybersecurity experts and programmers—and when you have a hammer, everything looks like a nail. They were largely looking at sophisticated, cyber-based attacks. But there are simple physical attacks, as we proved, that are easier to do and harder to prevent.*

The voting-machine companies never responded to the Argonne reports. “That’s not unusual,” says Johnston. “The manufacturers seem to be in denial on some of these issues.”