



Center For

**Information Technology Policy**

Princeton University

## Security Analysis of the Diebold AccuVote-TS Voting Machine

[Ariel J. Feldman](#), [J. Alex Halderman](#), and [Edward W. Felten](#)

**Abstract** This paper presents a fully independent security study of a Diebold AccuVote-TS voting machine, including its hardware and software. We obtained the machine from a private party. Analysis of the machine, in light of real election procedures, shows that it is vulnerable to extremely serious attacks. For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code; malicious code on a machine could steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could also create malicious code that spreads automatically and silently from machine to machine during normal election activities — a voting-machine virus. We have constructed working demonstrations of these attacks in our lab. Mitigating these threats will require changes to the voting machine's hardware and software and the adoption of more rigorous election procedures.

[Full research paper](#) [PDF]

[Executive summary](#)

[Frequently asked questions](#)

[Our reply to Diebold's response](#)

[Princeton e-voting studies](#)

[Demonstration Video](#)



**Hi-res video and downloads**

Princeton University - School of Engineering and Applied Science - Woodrow Wilson School