

Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

« “Hotel Minibar” Keys Open Diebold Voting Machines
Honest Election Workers »

Refuting Diebold's Response

Wednesday September 20, 2006 by Ed Felten

Diebold issued a response to our e-voting report. While we feel our paper already addresses all the issues they raise, here is a point by point rebuttal. Diebold's statement is in italics, our response in normal type.

Three people from the Center for Information Technology Policy and Department of Computer Science at Princeton University today released a study of a Diebold Election Systems AccuVote-TS unit they received from an undisclosed source. The unit has security software that was two generations old, and to our knowledge is not used anywhere in the country.

We studied the most recent software version available to us. The version we studied has been used in national elections, and Diebold claimed at the time that it was perfectly secure and could not possibly be subject to the kinds of malicious code injection attacks that our paper and video demonstrate. In short, Diebold made the same kinds of claims about this version — claims that turned out to be wrong — that they are now making about their more recent versions.

Normal security procedures were ignored. Numbered security tape, 18 enclosure screws and numbered security tags were destroyed or missing so that the researchers could get inside the unit.

This is incorrect. Far from ignoring Diebold's "normal security procedures", we made them a main focus of our study.

The tape and seals are discussed in our paper (e.g., in Section 5.2), where we explain why they are not impediments to the attacks we describe. The main attack does not require removal of any screws. Contrary to Diebold's implication here, our paper accounts for these measures and explains why they do not prevent the attacks we describe. Indeed, Diebold does not claim that these measures would prevent any of our attacks.

A virus was introduced to a machine that is never attached to a network.

This is irrelevant. Our paper describes how the virus propagates (see Sections 2.2.2 and 4.3) via memory card without requiring any network.

By any standard — academic or common sense — the study is unrealistic and inaccurate.

This is little more than name-calling.

For an academic evaluation, ask our academic colleagues. We'd be happy to provide a long list of names.

We demonstrated these problems on our video, and again in live demos on Fox News and CNN. Common sense says to believe your eyes, not unsubstantiated claims that a technology is secure.

The current generation of AccuVote-TS software — software that is used today on AccuVote-TS units in the United States — features the most advanced security features, including Advanced Encryption



Standard 128 bit data encryption, Digitally Signed memory card data, Secure Socket Layer (SSL) data encryption for transmitted results, dynamic passwords, and more.

As above, Diebold does not assert that any of these measures would prevent the attacks described in our paper. Nor do we see any reason why they would.

These touch screen voting stations are stand-alone units that are never networked together and contain their own individual digitally signed memory cards

As discussed above, the lack of networking is irrelevant. We never claim the machines are networked, and we explain in our paper (e.g. Sections 2.2.2 and 4.3) how the virus propagates using memory cards, without requiring a network.

Again, Diebold does not claim that these measures would prevent the attacks described in our paper.

In addition to this extensive security, the report all but ignores physical security and election procedures. Every local jurisdiction secures its voting machines — every voting machine, not just electronic machines. Electronic machines are secured with security tape and numbered security seals that would reveal any sign of tampering

Our paper discusses physical security, election procedures, security tape, and numbered security seals. See, for example, Sections 3.3 and 5.2 of our paper. These sections and others explain why these measures do not prevent the attacks we describe. And once again, Diebold does not assert that they would.

Diebold strongly disagrees with the conclusion of the Princeton report. Secure voting equipment, proper procedures and adequate testing assure an accurate voting process that has been confirmed through numerous, stringent accuracy tests and third party security analysis.

Every voter in every local jurisdiction that uses the AccuVote-Ts should feel secure knowing that their vote will count on Election Day.

Secure voting equipment and adequate testing would assure accurate voting — if we had them. To our knowledge, every independent third party analysis of the AccuVote-TS has found serious problems, including the [Hopkins/Rice report](#), the SAIC report, the [RABA report](#), the [Compuware report](#), and now [our report](#). Diebold ignores all of these results, and still tries to prevent third-party studies of its system.

If Diebold really believes its latest systems are secure, it should allow third parties like us to evaluate them.

This entry was posted on Wednesday September 20, 2006 at 8:00 am and is filed under [Security](#), [Voting](#). You can follow any responses to this entry through the [RSS 2.0 feed](#). You can [leave a response](#), or [trackback](#) from your own site.