Paperless E-Voting Fails Again

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Long-time readers may recall that I have inveighed against paperless electronic-voting (e-voting) machines for some time. In recent weeks there’s been more bad news for proponents of such systems – and for the future of democracy.

The basic problem is that e-voting machines that provide no paper audit trail are a disaster waiting to happen. Any error in such systems, including deliberate tampering, that alters the vote counts cannot, even in principle, be prevented from altering election results. For the time being, we need systems that produce a paper record the voter can compare with her vote; if the paper accords with her choice, she can then deposit the audit record in a secure repository for use in a recount if necessary.


Despite the efforts of the Diebold Company to prevent independent study of its e-voting products, the researchers were able to buy an AccuVote-TS machine and subject it to a thorough security analysis.

Dr Felten’s team found that malware inserted through a removable memory card with as little as one minute of access to the voting machine could cause all kinds of mischief such as switching vote counts or otherwise damaging the election results.

Diebold’s response “attributed to Dave Byrd, President, Diebold Election Systems,” attacked the study on specious grounds and was soundly refuted by Ed Felten in a riposte on September 20.

To hear an interview with Ed Felten on the “Weekend Edition” program for Saturday, September 23 by NPR’s Scott Simon about this report and the propaganda attack by Diebold, you can visit. The host raised many of the criticisms published in Diebold’s attack and Dr Felten responded convincingly to each of them.

I think that we in the United States should be following the example of the Australian government. There, e-voting machine code is open for inspection by all and has continued to be improved over the years since its introduction and implementation in voting machines. See for example a 2003 report by Kim Zetter in Wired entitled, “Aussies Do It Right: E-Voting.”

Programmers and security experts interested in supporting an open-source model for e-voting in...
the US (and elsewhere) can volunteer at the Open Voting Consortium <http://www.openvotingconsortium.org/>.

Make your vote count: don’t let proprietary, secret software undermine what little democracy we still have left.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.