Comments on "Review of Recent Information Security Issues Involving Maryland's Voting Technology" for the State of Maryland's Office of the Attorney General by M. Glenn Newkirk, InfoSENTRY Services, Inc.

by David L. Dill
Professor of Computer Science, Stanford University
Founder of the Verified Voting Foundation and VerifiedVoting.org
dill@cs.stanford.edu

April 9, 2006

I have recently obtained this report. The report it is not a security evaluation of the voting machines, nor a "study," nor even an opinion piece. It is propaganda, with the obvious intent of persuading Maryland to keep it's Diebold AccuVote-TS touch-screen machines. The only data or facts cited are from well-known publications -- and those quotations are chosen selectively in many cases to distort the truth.

I won't do a point-by-point rebuttal, but highlight some of the major problems.

1. The security discussion misses the point. It defines the "security" problem differently from the technologists and activists who have opposed the Diebold machines.

The demand for voter-verified paper records (VVPR) is driven by the desire to be able to observe election processes and independently audit the results of elections.

Paperless e-voting systems, such as the Diebold AccuVote-TS used in Maryland, thwart transparency by preventing people from observing the casting of votes and the handling of ballots, and thwart auditing by not having an independent records of the ballots.

However, from the perspective of transparency, the most important question is whether the machines are guaranteed to correctly record votes. Since there is no effective way to prevent design flaws or malicious behavior by the voting system, this is a lost cause without the increased transparency and auditability afforded by a VVPR, along with appropriate procedures and election laws.

The report doesn't explicitly state assumptions about the threat model, but the model is apparently that the attackers have no special access or knowledge of the machines. For example, the attacker could be a voter during the election. Other possible attackers are not considered, such as poll workers, elections office staff, warehouse guards, shippers, vendor employees such as programmers and system administrators, and intruders on

the vendor's computer networks.

The report does not discuss the possibility that malicious or erroneous software could be written by the programmers, or installed on the machines by a variety of different parties. It also presents no effective defenses against these attacks (which is not surprising, because there ARE no effective defenses against some of them).

2. The report's discussion of residual votes is deliberately confusing and distorted.

The discussion is confusing, because the residual votes have nothing to do with "Information Security Issues." For example, a dishonest paperless e-voting machine that changed non-votes to votes would have a residual vote rate of 0.

The distortion occurs because of selective quotation. Professor Charles Stewart III, whose work is heavily cited, has consistently found that precinct-count optical scan systems are extremely accurate, a fact that is not disclosed in Newkirk's paper. In fact, on p. 3, Newkirk quotes Stewart, but omits Stewart's previous sentence:

This finding is intriguing because in previous research (VTP 2001; Ansolabehere and Stewart 2005), we discovered that optical scanners tended to have the lowest residual vote rates and that DREs tended to have higher residual vote rates.

3. Results of previous security studies are cited in a misleading way.

Every competent study of the security of the Diebold AccuVote-TS has found computer security flaws that are not only extremely serious, but indicative of technical incompetence in computer security. Those studies include the Johns-Hopkins/Rice report in 2003, the SAIC and RABA reports commissioned in Maryland, and the recent report in California of the AccuVote-TSx AccuBasic interpreter. Indeed, these studies collectively form a stunning indictment of the security of these machines.

Here are a few of my favorite examples of security flaws: (1) The built-in pin numbers and cryptographic keys in the AccuVote-TS. Diebold was warned of these problems by Prof. Doug Jones in Iowa in 1997 or 1998, and the problems were still in the code to be discovered in the Johns-Hopkins/RABA report in 2003. The SAME crypographic key was STILL in the code this year, as was revealed in the California Secretary of State's evaluation of the Diebold interpreter, and (2) a member of the RABA "red team" who was able to gain control of a voting machine in a simulated election using a flexible keyboard that was wrapped around his arm.

However, although many of these studies are cited in this report, the report selectively quotes only the parts of the reports that sound complimentary.

Incredibly, Newkirk defends the AccuVote-TS on the grounds that it has had more security evaluations than the AutoMark. But, the AutoMark simply marks a paper ballot, like a pen or pencil. The result can be checked by anyone who looks at the ballot. So the AutoMark is nowhere near as security-critical as the AccuVote-TS.

The AccuVote-TS and -TSx have had many security evaluations because every one of those evaluations has discovered major security flaws. After each study, additional studies commissioned either to find out whether the flaws are fixed, or in the hope of invalidating previous studies. In each case (except Newkirk's essay), even more security flaws are found.

4. The author inappropriately minimizes the importance of the the "Hursti Hack".

On p. 4, Newkirk presents a silly analogy to make the point that the Hursti attack requires knowledge of the machine design. However, one of the most basic principles of computer security is that the security of the system should not depend on secrecy of the system design. Newkirk either does not know this, in which case is completely unqualified to be writing about security, or he is ignoring it, in which case he is being disingenuous.

Even so, it turns out that, Hursti did not have full details of the systems design, and had to "reverse engineer" the interpreter instructions in order to successfully demonstrate his attack.

Furthermore, Newkirk cites the California study without quoting the following defense of Hursti's work:

Harri Hursti's attack does work: Mr. Hursti's attack on the AV-OS is denitely real. He was indeed able to change the election results by doing nothing more than modifying the contents of a memory card. He needed no passwords, no cryptographic keys, and no access to any other part of the voting system, including the GEMS election management server.

In summary, Newkirk's essay is not a serious discussion of the technical or policy aspects of voting machine security, and is useless as a basis for policymaking on that question