c/o 3548 Beechwood Boulevard
Pittsburgh, Pennsylvania 15217-2767
412-421-0178

VoteAllegheny Analysis of the
Pro V&V iVotronic® Re-examination Test Protocol

Revision 3.2 of April 10, 2012

David A. Eckhardt, Ph.D.

Background

In Allegheny County, Pennsylvania, voters use equipment designed and sold by Election Systems & Software of Omaha, Nebraska (“ES&S”). Most Allegheny County voters cast their votes on iVotronic® touch-screen voting terminals; these machines are configured, and votes cast on them are tabulated, using a software suite called Unity™. The iVotronic voting terminal is used in twenty-five counties with between two and three million registered voters, making it one of the most widely used pieces of voting equipment in Pennsylvania.[1]

The iVotronic/Unity system was first certified by the Secretary of the Commonwealth in late 2005. As of early 2012 the Pennsylvania Department of State is conducting a re-examination of this equipment. This report attempts to analyze public information about the re-examination to characterize its scope. In particular, it is unclear, based on public information, whether the Department of State's re-examination will consider serious security vulnerabilities in the iVotronic and Unity software which have been publicly characterized by official investigations in other states.

Timeline

On December 22, 2005, Secretary of the Commonwealth Pedro A. Cortés certified the ES&S iVotronic touch-screen voting system for use in Pennsylvania. This certification applied to iVotronic software version 9.1.2.0 and Unity software version 3.0. On April 7, 2006, Secretary Cortés certified an updated version of the system, using iVotronic software version 9.1.4.1 and Unity software version 3.0.1.0.

On September 13, 2006, Ariel J. Feldman, J. Alex Halderman, and Dr. Edward W. Felten of Princeton University released a paper[2] describing security vulnerabilities in the Diebold[3] AccuVote-TS touch-screen voting terminal. As part of their work they developed a virus which was capable of transferring votes from one candidate to another and propagating among voting terminals via infected memory cards. Because the ES&S iVotronic and the Diebold Accuvote-TS use different hardware and software, the AccuVote-TS virus cannot attack iVotronic machines. However, to the extent that iVotronics are structurally similar to the AccuVote-TS and contain vulnerabilities similar to the ones exploited by the Princeton team, it is plausible that individuals with similar background and skills could implement a similar attack.

The results of the November 7, 2006 general election in Florida's Congressional District 13 were anomalous. In particular, in Sarasota County, no vote was recorded in the U.S. House race for approximately 18,000 voters. In December of 2006 the Florida Department of State commissioned an expert review of the iVotronic software in order to investigate whether “[...] flaws, vulnerabilities or anomalies […] potentially caused, contributed or otherwise created the higher than expected under-vote rate in the District 13 Race.” A team of eight investigators published a report, titled “Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware,” on February 23, 2007. The primary finding of the investigators was that “the iVotronic firmware, including faults that we identified, did not cause or contribute to the CD13 undervote.” However, the investigators also reported finding serious security vulnerabilities in version 8.0.1.2 of the iVotronic firmware. Their report noted

[1] Based on 2008 numbers provided by VotePA.us, 2.6 million voters reside in counties which primarily use iVotronics; 300,000 voters in Chester County choose between paper ballots and iVotronics.

[2] Feldman, Halderman, and Felten: Security Analysis of the Diebold AccuVote-TS Voting Machine, September 13, 2006.

[3] Diebold later sold its Diebold Election Systems subsidiary to ES&S in 2009.

that "Fixing these vulnerabilities is likely to be non-trivial because it requires fixing a flaw in the architecture and architectural flaws tend to be more difficult to fix once they are implemented."

In late 2007, Jennifer Brunner, the Secretary of State of Ohio, commissioned an in-depth study of the voting systems then used in Ohio. A team of 23 voting-system and computer-security experts from The Pennsylvania State University, The University of Pennsylvania, WebWise Security, and The University of California at Berkeley investigated, over the course of nine weeks, the software source code of the systems used in Ohio and published a report, titled "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing," on December 7, 2007. The EVEREST team studied versions 9.1.6.2 and 9.1.6.4 of the iVotronic firmware. The executive summary of the investigation of ES&S equipment states, "Our analysis suggests that the ES&S Unity EMS, iVotronic DRE and M100 optical scan systems lack the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions. Exploitable vulnerabilities allow even persons with limited access – voters and precinct poll workers – to compromise voting machines and precinct results, and, in some cases, to inject and spread software viruses into the central election management system [...] These vulnerabilities arise from several pervasive, critical failures of the ES&S system […] ."

The substantial and disturbing information about iVotronic and Unity vulnerabilities contained in the Florida and Ohio reports was uncovered and published after Pennsylvania's certification of the iVotronic/Unity system. A naïve interpretation of software version numbers would place the software used in Pennsylvania between the Florida and Ohio software in a plausible development timeline. Because some vulnerabilities were reported by both the Florida and Ohio teams, it is plausible that these vulnerabilities are present in the software used in Pennsylvania. In short, it would appear only prudent to investigate whether the specific serious vulnerabilities identified in the Florida and Ohio reports are present in Pennsylvania – especially since some of the EVEREST investigators are Pennsylvania residents. Note that the iVotronic vulnerabilities described in the Florida and Ohio reports are similar in structure and severity to the ones exploited by the Princeton team to successfully attack the AccuVote-TS.

On February 22, 2012, Pro V&V of Huntsville, Alabama, a contractor for the Pennsylvania Department of State, produced a document entitled "Commonwealth of Pennsylvania Test Protocol for Re-examination of iVotronic Touch Screen Voting System Version 9.1.4.1 and Unity Software Version 3.0.1.0". This document was used to guide a re-examination of the iVotronic/Unity voting system by Pro V&V which began in Harrisburg on February 29, 2012.

This report analyzes the Pro V&V iVotronic test protocol document to evaluate the likelihood that testing carried out according to that protocol will detect plausible (e.g., previously demonstrated) iVotronic and/or Unity vulnerabilities if they are present in Pennsylvania.

Report Outline

We will begin with several observations and questions about parts of the Pro V&V document which we believe bear on the scope of the re-examination. Then we will discuss several technical-detail questions raised by the document. Finally, we will conclude with a brief summary of possible implications for the voters of Allegheny County.

Re-examination Scope

Our review of the Pro V&V document raises the following scope-related issues.

1. Text at the top of page 1 states that this is a test of the previously certified software (version 9.1.4.1) rather than a later version submitted by ES&S. Thus, it appears reasonable and prudent for an examination to consider the issues raised in the Florida and Ohio reports.
2. However, Section 3 ("Test materials") does not list source code as among the "materials made available to Examiner for the re-examination." While it would be *possible* to investigate some of the issues raised in the Florida and Ohio reports by using object-code decompilation or "black box" penetration testing, analysis based on source code is generally less laborious and more fruitful. Because the experts who prepared the Florida and Ohio reports worked from source code, replicating their investigations would probably be most straightforward if it were based on analyzing source code. The report of the examiner appointed by the Secretary for the November, 2005 iVotronic/Unity examination indicates that source code was made available for that examination, so presumably it could be made available for the current re-examination as well.
3. Table 3.2 on page 6 lists "Third Party Test Reports." However, it does ***not*** list the Florida report or the Ohio report. Again, while it would be *possible* to fully investigate all security vulnerabilities without reference to this prior work, it seems unlikely that this would be the most fruitful approach. It is plausible that the Secretary's examiner could gain access to not only the public portions of the Florida and Ohio reports but also additional material for which distribution was limited.
4. Text in Section 5 (page 7) appears to indicate that some or all of the verification that the system under test is "capable of absolute accuracy" will be done off-site. The scope of this off-site work, and the eventual reporting on it, is somewhat unclear.
5. The meaning of text on "Penetration Analysis" (page 89) is not entirely clear to this author. In particular, the protocol document states that "Depending on the scope of this project this [testing] may be performed by a third-party expert." It is not obvious when the identity of the tester was or will be decided. The fifth step of this test is described as "attempt to bypass the security environment by various methods such as disabling the printer, removing power, and any other means to try and compromise the votes." The extent of "any other means" is not clear.

Overall, after reviewing the protocol document a key question remains open: will this re-examination consider serious security vulnerabilities identified in 2006 and 2007 by voting-system experts (including the original Pennsylvania iVotronic/Unity examiner)? If so, will the investigation be carried out using similar methods?

Technical Details

The following questions are of a more detailed technical nature and may indicate limitations on the detail level of the document rather than potential limitations of the re-examination. It would be helpful if the examiner's final report could clarify these issues.

1. Table 2.3 on page 4 appears to indicate that PEB's are "optional" and doesn't list revision numbers for hardware or software. To this author's knowledge, PEB's are *not* optional; meanwhile, based on the Florida and Ohio reports, there is reason to be believe that a PEB

running uncertified firmware could be used to compromise the integrity of an iVotronic running firmware version 9.1.4.1.

2. Test case "01-25 PS 3031.7(1) Voter Secrecy (ADA Vote)" (pages 62-64) investigates whether a naked-eye observer near an iVotronic being operated in ADA mode can see a voter's vote as it is being selected. Naked-eye observers are indeed an important threat to voter secrecy, but there are others. For example, in 2006 Dutch investigators discovered that a "NEDAP ES3B" direct-recording electronic voting machine used in the Netherlands leaked radio-frequency signals in a fashion that allowed a remote eavesdropper to determine a voter's selections.[4] In 2007 they wrote "It is remarkable that nobody appears to have ever tested for any spurious emissions [...]"; hopefully, their experience is being used to improve voting-system certifications taking place after their publication.
3. Again with reference to "Penetration Analysis" (page 89), the sixth step is "verification of password security management at all levels." Based on the text it is not clear whether the re-examination will test whether iVotronic software version 9.1.4.1 is vulnerable to the "factory-test PEB"/"quality-assurance PEB" back-door in the password system which was reported by the Florida team and reproduced by the Ohio team.

Possible Implications

The current re-examination of the iVotronic/Unity system has the potential to serve as a vehicle for improving system security, public confidence, or both. The integrity of elections in Pennsylvania stands to be improved by a better understanding of the strengths and weaknesses of the systems in use. Where weaknesses are identified, it may be possible to mitigate some through software upgrades and/or increased deployment and operational security. In some cases new information might make it necessary to decertify some systems (as has happened in Pennsylvania and other states).

At present it is not clear from the Pro V&V protocol document whether the current re-examination will take into account all relevant information and investigative techniques.

Whatever the outcome of the re-examination is, it is important to public confidence that the process be based on the best available information and investigative methods. Hopefully this analysis can help ensure that the examiner's final report and the Secretary's eventual certification decision are based on a strong foundation.

About the author

Since 1997 David A. Eckhardt has served as an appointed Judge of Elections in Mt. Lebanon, Pennsylvania. This position entails managing a single polling place serving approximately 800 registered voters.

Since 2003 Dr. Eckhardt has taught Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. His areas of specialty are operating systems and computer networks.

These two areas of activity, formerly independent, began to overlap in 2006 when Allegheny County voters began to vote using computers. Since then Dr. Eckhardt has contributed to various reports as a

[4] See Gonggrijp and Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective," Proceedings of EVT '07, USENIX, 2007 and also "voting computer tempest attack" [sic], http://www.youtube.com/watch?v=B05wPomCjEY

member of VoteAllegheny and as a member of the Allegheny County Citizens' Election System Advisory Panel. In the fall of 2011, on behalf of the Venango County Board of Elections, he participated in an investigation of the auditability of elections carried out on iVotronic voting terminals and tabulated with Unity. This work gave rise to a document entitled “Audit Analysis of the Venango County 2011 Municipal Primary - Initial Report.”

About VoteAllegheny

VoteAllegheny is a non-partisan volunteer election integrity group. More information is available at www.VoteAllegheny.org.