Technical Reasons to Question St. Louis County Voting Results

By Missourians for Honest Elections

Technical Concerns with iVotronic Voting Machines

The electronic voting machines used by St. Louis County (the ES&S iVotronic) since 2006 have a number of documented vulnerabilities. In elections other than a general election, these machines typically collect 80% of the votes in the county. The other 20% are paper ballots that are scanned into the system. The problems outlined below have all been reported to the St. Louis County Board of Elections.

- Security Vulnerabilities of the ES&S iVotronic DRE

    - **Weak Password Protection**: An analysis by Florida State University in 2007 concluded that password protection is very weak:

        "Our judgment is that the password mechanisms on the iVotronic are poorly conceived and poorly implemented. The consequence is that the passwords by themselves do not do a good job of preventing unauthorized individuals from accessing critical system functions.

        Finally, these passwords can all be bypassed using a special type of PEB, called a Factory Test PEB. When a PEB is inserted, the iVotronic machine queries the PEB to ask it what kind of PEB it is, and the PEB returns a single byte indicating what type of PEB it is. A Factory Test PEB identifies itself by returning a special single-byte value. This special value is hard-coded into the iVotronic code. Anyone who knows the special single-byte value, has access to a PEB and is able to program the PEB could construct a PEB that identifies itself as a Factory Test PEB. When a Factory Test PEB is present, all password checks are bypassed: in places where the user would normally need to enter a password, the password check is bypassed, the machine functions as though the correct password had been entered, and a log entry is appended to the event log as though the user entered the correct password. This undocumented backdoor poses a risk of unauthorized access to critical system functions, because it provides a way that a malicious individual could bypass the password checks by tampering with a PEB."

        Report by Florida State University for the Florida Department of State, "*Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware*," page 67 (see Florida Sec. of State website for online copy of report at: http://election.dos.state.fl.us/reports/pdf/FinalAudRepSAIT.pdf)

        Note that after the analysis the State of Florida got rid of the machines.

    - **Failed Systems Software**: An extensive analysis of the iVotronic called the Everest Report was completed for the Ohio Secretary of State in 2007 by three teams of computer experts from the University of Pennsylvania, Pennsylvania State University, and WebWise Security (a computer security consulting firm). The teams came to the following conclusions about the iVotronic DRE and its supporting systems:

"This part of the EVEREST report evaluates the ability of the ES&S Unity EMS, iVotronic DRE, and M100/M650-based optical scan voting systems to conduct trustworthy elections. The review team was provided access to the ES&S source code and election equipment. The reviewers studied these materials in order to identify security issues that might be exploited to affect an election. As part of that analysis, the reviewers were asked to identify, where possible, practices that limit or neutralize the impact of discovered issues.

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. Such compromises render the election result subject to subtle manipulations – potentially across election cycles. These vulnerabilities arise from several pervasive, critical failures of the ES&S system:

- ***Failure to protect election data and software*** *– The firmware and configuration of the ES&S precinct hardware can be easily tampered with in the field. Virtually every piece of critical data at a precinct—including precinct vote tallies, equipment configuration and equipment firmware—can be compromised through exposed interfaces, without knowledge of passwords and without the use of any specialized proprietary hardware.*

- ***Failure to effectively control access to election operations*** *– Access to administrative and voter functions are protected with ineffective security mechanisms. For example undocumented "quality assurance" hardware tokens that bypass password checks are easily forged using inexpensive commodity devices such as palmtop computers. Central back-end election management software is vulnerable to attacks that exploit coding and design errors and that can be triggered from data sent from the field.*

- ***Failure to correctly implement security mechanisms*** *– Many of the most serious vulnerabilities in the ES&S system arise from the incorrect use of security technologies such as cryptography. This effectively neutralizes several basic security features, exposing the system and its data to misuse or manipulation.*

- ***Failure to follow standard software and security engineering practices*** *– A root cause of the security and reliability issues present in the system is the visible lack of sound software and security engineering practices. Examples of poor or unsafe coding practices, unclear or undefined security goals, technology misuse, and poor maintenance are pervasive. This general lack of quality leads to a buggy, unstable, and exploitable system.*

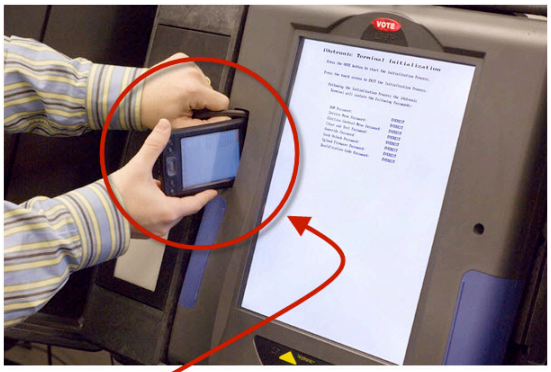
We believe the issues reported in this study represent practical threats to ES&S-based elections as they are conducted in Ohio. It may in some cases be possible to construct procedural safeguards that partially mitigate some of the individual vulnerabilities reported here. However, taken as a whole, the security failures in the ES&S system are of a magnitude and depth that, absent a substantial re-engineering of the software itself, renders procedural changes alone unlikely to meaningfully improve security."

The Everest Report was created by three teams of computer experts at the request of the Ohio Secretary of State in the winter of 2007 as part of the Everest Voting Systems Analysis Project. The publication title was "*EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*." The quote above is from page 29, Chapter 4, "The ES&S Executive Summary". [Bolding emphasis above was added by the authors of this paper]. A complete electronic copy of the 316 page report can be obtained by contacting the authors of this white paper.

- **Hole in ES&S Election Management Software.** Duncan Buell, Professor in the Department of Computer Science and Engineering at University of South Carolina found in an analysis of all the electronic records of a South Carolina election that several counties failed to load the results of DREs that were taken into the field and whose database contained valid votes for the election. Professor Buell postulates that this probably happened because there is no reporting function in the Election Management Software from ES&S that ties out the results with the databases of electronic ballot records.

- **iVotronic Physical Vulnerabilities**

  Easy private access to DRE controls. Access to the control system of an iVotronic is on the side of the machine facing the voter, obscured from poll worker oversight. As documented in the Everest Report the only equipment needed to gain access to the internal workings of the DRE during an election is a Palm Pilot and a magnet. Further, using a Palm Pilot's infra-red port the software needed to emulate a PEB can be wirelessly and invisibly downloaded from a distance from an activated PEB in the polling place. The photo below shows a Palm Pilot and magnet being used to bring up the machine's main internal operations menu.



The PEB port is easily available to the voter…

Easy access to DREs before Election Day. Because St. Louis County has to distribute as many as 1800+ DREs to approximately 450 polling places around the county, the DREs must be delivered several days in advance of the election. Potentially, they are delivered several weeks before an election. Schools, public buildings, and churches do not typically have high levels of security, making access to a machine outside of the public eye relatively easy. The Everest Report suggests that all that is needed to electronically take over an election is access to a single one of the 1,800 DREs prior to (or during) Election Day where a virus can be planted that will move itself to the central tabulator system to control election outcomes.

Handling of Broken Seals on DRE Containers Inadequate. There is a standard procedure that is followed when the tamper seals are broken on DRE containers on Election Day. The procedure seems to be that the technician runs a "Logic and Accuracy" test and—provided the machine passes the test—then releases the machine to the poll workers to be used in the election. If the "Logic and Accuracy" test is built into the software—as is highly likely—then any malicious program would be certain to look for this test and allow the test to proceed with the original software code. In other words, malicious code would likely be invisible to a built-in "Logic and Accuracy" test.

- **No Public Review of Software**

Public Access to Source Code Not Available. Access to source code running the DREs is only available to Missouri public officials under the following very limited set of conditions. (N.B. Suspicion of electronic election fraud is not one of the reasons for public access to the source code.)

> **"...***Missouri will, within seven (7) days of the occurrence of one of the following events, receive full access to the source code and unlimited rights to continue using and supporting the software at no cost to the state or the agency should the manufacturer:*
>
> 1. *"Become insolvent; or*
> 2. *Make a general assignment for the benefit of creditors; or*
> 3. *File a voluntary petition of bankruptcy; or*
> 4. *Suffer or permit the appointment of a receiver for its business or assets; or*
> 5. *Become subject to any proceeding of bankruptcy or insolvency law, whether foreign or domestic; or*
> 6. *Wind up or liquidate its business voluntarily or otherwise and the state has reason to believe that the vendor will fail to meet future obligations; or*
> 7. *Discontinue support of the provided products or fail to support the products in accordance with its maintenance obligations and warranties;"*
>
> From the Secretary of State's Code of State Regulations, 15 CSR 30-10.020.

Tainted initial Federal Code Review. At the time when the iVotronic voting machine currently in use in St. Louis County was submitted to various "independent" agencies for verification that its code worked and contained no malicious subroutines, there were numerous published reports that the testing process had broken down with some labs issuing certifications without doing any testing. Following is a NY Times description of the testing process the iVotronic was subjected to.

> *"But there is, to begin with, a stunning lack of transparency surrounding this process. Voters have a right to know how voting machine testing is done. Testing companies disagree, routinely denying government officials and the public basic information. Kevin Shelley, the California secretary of state, could not get two companies testing his state's machines to answer even basic questions. One of them, Wyle Laboratories, refused to tell us anything about how it tests, or about its testers' credentials. 'We don't discuss our voting machine work,' said Dan Reeder, a Wyle spokesman.*
>
> *Although they are called independent, these labs are selected and paid by the voting machine companies, not by the government. They can come under enormous pressure to do reviews quickly, and not to find problems, which slow things down and create additional costs. Brian Phillips, president of SysTest Labs, one of three companies that review voting machines, conceded, 'There's going to be the risk of a conflict of interest when you are being paid by the vendor that you are qualifying product for.'*
>
> *It is difficult to determine what, precisely, the labs do. To ensure there are no flaws in the software, every line should be scrutinized, but it is hard to believe this is being done for voting software, which can contain more than a million lines. Dr. David Dill, a professor of computer science at Stanford University, calls it 'basically an impossible task,' and doubts it is occurring. In any case, he says, 'there is no technology that can find all of the bugs and malicious things in software.' "*
>
> NY Times opinion piece, "*Who Tests Voting Machines?", May 30th, 2004*
>
> (N.B. There is no publicly available information to suggest that the software in the machines used in St. Louis County has ever been subjected to any kind of rigorous public review.)

Missouri's Certification of DREs Inadequate. According to a conversation with a computer expert on the public committee assigned to certify the acceptability of DREs for purchase in Missouri, his instructions were to make sure that certain encryption capabilities were in the software and that the CDs didn't contain the "...sonnets of Shakespeare rather than computer code [sic]." The committee only met for a couple of days as part to review the specifications of available machines in Missouri's rush to certify them for purchase in 2005. There was no way he could have done even a cursory review of the tens of thousands of lines of

code in each of the several systems being considered at the time.

- **No Public Commitment by Manufacturers to Accuracy of Results**

  - Manufacturers Not Required to Certify their Machines Produce Accurate Results. Following is the certification that manufacturers of DREs are required to swear to as part of the certification of DRE equipment.

    " *Manufacturer's Certification Statement*

    I, _____,[electronic voting systems company] do hereby certify to _____, Secretary of State of Missouri that the _____ [name of equipment] electronic voting system will permit in accordance with section 115.225, RSMO:

    1. *Voting in absolute secrecy;*
    2. *Each elector to vote at any election for all persons and offices for whom and for which s/he is lawfully entitled to vote;*
    3. *The automatic tabulating equipment to be set to reject all votes for any office or on any measure except write-in votes when the number of votes exceeds the number the voter is entitled to cast;*
    4. *Each elector to vote for as many persons for an office as s/he is entitled to vote for;*
    5. *Each elector to vote for or against any questions upon which s/he is entitled to vote; and to vote, by means of a single device, where applicable, for all candidates of one (1) party or to vote a split ticket as s/he desires;*
    6. *Each elector, at presidential elections, by one (1) punch or mark, to vote for the candidate of that party for president, vice-president and their presidential electors; and*
    7. *The _____ electronic voting system complies with all other requirements of the election laws of the state of Missouri where they are applicable. (Briefly describe the type of electronic voting system provided by _____ the means by which it meets the requirements of provisions 1.-6 and list the areas in which the system is in use.)*

    I do hereby certify that the above information is true and accurate this _____day of _____, 20__. _____(President)"

    From the Missouri Secretary of State's Code of State Regulations (CSR) 15 CSR 30-10.020 "Certification Statement for New or Modified Electronic Voting Systems."

    It's notable that this statement does not required the manufacturer to give any assurance that the machines will produce accurate results.

- **Impossible Software Chain of Custody.**

  - Software Updates Are Easy Point of Entry for Malicious Code. Updates to the software in the approximately 1,850 DREs used by St. Louis County involve loading software into each machine. It is impossible for the individual loading the software to know with any

certainty that the code being loaded is the original code from the manufacturer. Further, it is impossible for any supervisor to know that an employee loading new versions of or fixes to manufacturer's software is loading the correct code. As shown by the Everest Report above, all that is needed to take over a county's election is to put malicious code into one DRE. The poor design of the system assures that a virus targeted at the central tabulating computer for an election can move on its own from a DRE to the central computer.

- **No Audit Capabilities**

  - Paper Tape Offers No Assurance of Voter Verification. In fact, the number of St. Louis County voters who actually do verify the tape is low, as is evidenced by reports in the Tech Maintenance Logs of paper tape jams that continued for hours while the DRE was in use, with no voters even noticing the jam. The lack of voter verification of the tape is also supported by our own informal survey of voters exiting the polls during the early voting period of one general election: less than half of the voters said that they did. Moreover, during one general election there were over 35 items on the ballot. Any reasonable estimate of the amount of time needed to vote such a ballot and to also verify the paper would not have allowed for more than about 90 persons to vote in the course of Election Day on a single machine. However, the average voters on DREs during this election was over 125.

  - The Board of Elections' Position on Voter "Verifiable" Tapes Inconsistent With Public Expectation. In a video of a conversation at a public hearing at the Board of Elections on 21 September 2010, the then leading Director of Elections expressed the view that as long as the system they offer gives voters a chance to verify their votes on a paper record, the Board has done its job. It was his opinion if voters choose not to check the record, this was not a matter of concern for the Board, even though this tape is supposed to be relied on for audits and recounts.

  - Required Randomness in Audits Not Possible.

    > ***"15 CSR 30-10.110 Manual Recount*** *- ...(2) Prior to the certification of the election results, the accuracy certification team shall randomly select not less than five percent of all election precincts through the use of a random drawing, but not less than one (1) precinct, in order to conduct a manual recount of selected contested races and ballot issues in the selected precinct(s)."*
    >
    > From the Missouri Sec. of State's Code of State Regulations, 15 CSR 30-10.110

    The St. Louis County Board of Elections technician logs from the November 2012 election show that there were 150 paper jams, many of which were reported as "serious" or "major." Some jams lasted for hours and resulted in the loss of any paper record of the votes during the jam. Discussions with the Directors of the Board of Elections indicate that if a machine has a damaged voter verifiable paper tape (VVPT), and the tape is selected for the required random audit mentioned above, a new "random" selection is made to find a VVPT that is not damaged. A procedure such as this invalidates the randomness

requirements for audits.

- Election Audit Assumes Software Worked Correctly. Every audit of results from an electronic vote collecting and vote tabulating machine starts from the assumption that the simple "Logic and Accuracy" test is sufficient to prove that the software works. The information above documenting the vulnerabilities of the system demonstrates that making that assumption is not reasonable.

- **Election Process Lacks Reasonable Public Oversight**

  - No electronic records of the election are available to the public.

    "Ballots and records to be kept twenty-two months, may be inspected, when.

    115.493. The election authority shall keep all voted ballots, ballot cards, processed ballot materials in electronic form and write-in forms, and all applications, statements, certificates, affidavits and computer programs relating to each election for twenty-two months after the date of the election. During the time that voted ballots, ballot cards, processed ballot materials in electronic form and write-in forms are kept by the election authority, it shall not open or inspect them or allow anyone else to do so, except upon order of a legislative body trying an election contest, a court or a grand jury. After twenty-two months, the ballots, ballot cards, processed ballot materials in electronic form, write-in forms, applications, statements, certificates, affidavits and computer programs relating to each election may be destroyed. If an election contest, grand jury investigation or civil or criminal case relating to the election is pending at the time, however, the materials shall not be destroyed until the contest, investigation or case is finally determined."

    Missouri General Statutes, 115-493

    The permission to destroy the records at the exact moment that they are no longer prohibited from public viewing effectively prohibits detailed public review of election operations. As interpreted by the St. Louis County Board of Elections, this statute prevents public access to any electronic records generated by the DREs during an election and to any reports based on those records.

- **iVotronic Mechanical Failures in St. Louis County**

  - The St. Louis County Board of Elections' "Tech Maintenance Records" from every major election since the DREs were purchased contain reports of serious DRE technical difficulties. Among the many DRE problems that the County's technicians have continually reported are such things as blank screens, frozen screens, and "screen calibration problems," including many cases in which voters said that a vote for one candidate appeared as a vote for another on the DRE screen. Our most recent review of these logs (from the November 2012 Election) found 386 reports of problems that occurred with the iVotronic machines that required the help of a technician. This includes 15 reports of an

iVotronic changing a voter's selection, or in some other way not allowing the voter to vote as desired. The logs also contain 218 reports of printer problems, including the 150 paper jams noted above. In addition, they contain 8 reports of low battery voltage, which—as the following evidence suggests—may cause the iVotronic to unreliably record internal data.

The Florida Fair Election Coalition, in its investigation of high undervotes in a Florida Congressional race that was conducted on ES&S iVotronic machines in 2006, noted that

> *"[they] found that low battery machines [in Charlotte County, Florida] had a combined undervote rate of an astonishing 31.25 percent."*

Source: Sarasota's Vanished Votes: An Investigation into the Cause of Uncounted Votes in the 2006 Congressional District 13 Race in Sarasota County, Florida," By Susan Pynchan and Kitty Garber, Florida Fair Election Coalition, page 37.

St. Louis County's Board of Elections must also have concerns about low battery levels. Even though during the election the machines are all daisy-chained to a regular electrical outlet, the technicians' log documents that much of the technicians' time during Election Day is spent checking battery levels.

- **iVotronic Failures Elsewhere**

  - Significant Under-votes in Five Florida Counties. In the November 2006 elections in Sarasota Florida the ES&S iVotronic machines used at all the polling places showed that there were roughly 18,000 undervotes (almost 13% of the voters on Election Day) in one highly contested congressional race. In four other counties in this district (three that didn't have iVotronic machines) the undervotes average lower than 3.5%. The resulting brouhaha gave a national black eye to Florida's elections, again. What never came to light in the national media was that there were five other counties that used iVotronic machines in Florida on that Election Day that had similar (or worse) undervotes for the State's Attorney General race:

County	Polling Undervote %	Absentee Undervote %
Broward	11.02	1.99
Charlotte	24.90	2.69
Lee	21.01	2.38
Miami-Dade	9.64	5.91
Sumter	24.96	3.21

All of these counties used ES&S iVotronics. Florida subsequently dropped use of DREs in favor of paper ballots that were scanned into electronic systems.

Data above from research done by the Florida Fair Elections Coalition and published in a report titled, " A Look at Extraordinary Undervote Rates On the ES&S iVotronic - Part 1." The report can be found at the coalition's website, http://www.ffec.org/CenterReports.htm .

  - Democratic Primary for US Senate Seat in South Carolina. A 2010 US Senate primary race for Democratic candidates in South Carolina resulted in a landslide for the candidate

who had no public service experience, no name recognition, no platforms, and made no public appearances before the vote. Further, the absentee ballots ran heavily in favor of the losing candidate while the Election Day voting—exclusively on ES&S iVotronic machines—went to the winning candidate, Alvin Greene.

Summary

The information provided above paints a clear picture of equipment that is vulnerable to hacking, subject to high levels of mechanical failure, impossible to audit, and likely the cause of election failures in other states. The question is, why are we still using it, when the cheaper, safer, more transparent alternative—paper ballots scanned into an electronic system—is easily available?

For questions please contact one of the coalition members below:

Phillip Michaels, (314) 862-3217, phillipmichaels@sbcglobal.net
Cynthia Richards, (314) 630-3916, crichar03@yahoo.com