Electronic Voting Machines in South Carolina

A Position Paper

Duncan Buell and Carter Bays

19 November 2004

Introduction

The state of South Carolina has recently embarked, with the help of Help America Vote
Act (HAVA) funding, on a plan to replace all voting machines in the state with a single
electronic machine. The machine chosen was the iVotronic machine from Election
Software and Systems (ESS). Use of these machines in the 2004 election was limited to
select counties that were felt to have distinctly suspect machines in place. The plan is
that by 2008, if not by 2006, all voting in the state will take place using these machines.

We start by assuming that there are four risks associated with electronic voting machines,
not all of which are unique to electronic equipment.

1. Deliberate attack: There is the risk that deliberate changes to hardware and/or
   software could compromise the election process by returning false or incorrect
   results or by disrupting the election process as it took place.

2. Software bugs and misconfigurations: There is the risk that accidental errors or
   unintended changes could compromise the election process by returning false or
   incorrect results.

3. Human error: There is the risk that the system is reliable in a controlled testing
   environment but that as deployed in the tumult of an election it will fail to

function properly, due to human error, and a disruption of the election process would follow.

4.   Loss of faith: There is the risk that the system will be viewed as suspect by voters and thus that voter participation in the electoral process will be diminished.

It is a basic fact that elections are unique events. They cannot be simulated in advance. Their detailed outcomes are largely unknown. They are one-time events that cannot be replayed. Just as NASA cannot perform an actual test of a spacecraft landing through a Martian atmosphere onto Martian gravity, no election commission can test an election system in advance under completely realistic situations. As such, then, the machines used in elections require engineering standards with at least the rigor we would expect for remote spacecraft.

We also admit in advance that no system will be perfect. Some arguments have been made that direct-recording electronic (DRE) systems are acceptable because they are more reliable than the systems they replace [WILLIAMS]. If this argument is true, it is nonetheless only half the story. If in addition to a potential greater reliability one also assumes a much greater potential risk, then this risk must be factored into policy decisions. From what we know of the electronic systems available, we believe the current risk is much too high to be acceptable. The systems are inherently insecure; it will be a complicated process to make them secure; and we expect that few election officials, especially at the local levels, will be able to maintain the security and reliability that voters have the right to expect.

The first author has participated in two discussions with the South Carolina State Elections Commission (SCSEC), one of which included a telephone conference call with the vice president for technology of ESS, Mr. Ken Carbullido. Based on this and on a review of the documentation available (the assessments conducted for the states of Maryland and Ohio, news reports and their rebuttals, papers from others and their rebuttals, etc. [JONESB, OHIOA, OHIOB, OHIOC, RABA, VOTERSUNITE]) we believe strongly that all four risks exist in South Carolina.

In what follows, we will address these risks. We will not, however, ask specific questions, or deal with the election process in the abstract, or address the risks individually. Instead, we will use our understanding of the ESS iVotronic that is in the process of being purchased for the entire State of South Carolina and our understanding of the operational process of elections in South Carolina. We intend to expose the risks we see with the system as it seems to be implemented in South Carolina and take our concern over those risks as a springboard for suggestions as to what must be done to make the election process reliable and trustworthy.

Full and Complete Disclosure Is Necessary

A very large part of the alleged security of the ESS system comes from the fact that ESS uses proprietary software and hardware for the machines. The system does not use Windows or Linux but rather a vendor-written operating system. The precise details of the hardware are proprietary. The suggestion that this is a "feature" of security has

certainly been made on the ESS websites as well as the SCSEC websites. In an attempt to quiet fears about the new machines, the SCSEC on its www.scvotes.org website lists as one of three "key features" of the ESS machines that it has a "proprietary Personal Electronic Ballot device" (PEB).

Security through obscurity is completely unacceptable [FARKAS, RABA, SCHNEIER]. The security of a system must not be premised on the notion that adversaries will not penetrate the physical and operational security of the institution, obtain a copy of the device, and reverse-engineer it. Security must begin with the premise that in spite of an adversary's having full knowledge of the hardware and software in the system, the protocols, cryptography, authentication, etc., provide by themselves all the security needed. The system should be secure and reliable even if, armed with a complete software listing and schematic of the hardware, the ESS chief engineer were to change stripes and become an adversary.

We argue that in an operational setting, with equipment distributed to hundreds or thousands of precincts statewide, it is unlikely that local officials will have the understanding of computer security necessary to realize that the proprietary nature of the hardware and software ought not to be taken as any indication of security. Even at the SCSEC, this did not seem to be understood.

If security through obscurity is to be a primary factor in alleging the existence of a robust and reliable system, then protection of that obscurity through physical and operational

security should become a primary mission of both the vendor and the election officials. If the security and reliability of elections is to depend on the inability of an adversary to obtain any information about the voting machine, then all devices that are part of that machine need to be secured throughout their manufacturing process and their use at the state and local level.

This level of physical security, however, is clearly not happening. In the first author's visits to the SCSEC, it appeared that the hardware was available, unsecured, in common areas, over extended periods of time. It did not appear to the first author that it would have been impossible to walk away with the handheld PEB that controls the voting process in an ESS machine, work overnight on reverse engineering the device, and then return it in the morning. We admit that this would not necessarily be an easy task, but we would be astonished to learn that all PEBs in all precincts in the country using them have been completely secured for their entire life span. Mr. Carbullido from ESS, when asked the direct question as to whether all devices were numbered and accounted for throughout their manufacture, could not say that they were.

We must assume, therefore, if we are to be serious about security, that the hardware to be used in South Carolina elections is completely known to any and all interested but unauthorized parties. We argue that the physical security necessary to protect a system based on proprietary hardware and software is impossible to guarantee. And even if it were possible to guarantee in South Carolina, it is unlikely to be guaranteed nationwide, perhaps even worldwide.

Our conclusions are based on an examination of the nature of the ESS equipment with its heavy reliance on obscurity as the primary contributor to its security and on an estimate of the concomitant level of physical security with which the devices would need to be maintained. We contrast this with the likelihood that the necessary level of security would in fact be maintained, and we conclude that any reliance on proprietary software or on proprietary hardware specifications is inadvisable. We recommend, therefore, that all hardware specifications and all software be publicly available. This full and public disclosure, permitting extensive scrutiny, seems absolutely necessary with regard to the software. It has been a hard-knocks lesson learned over fifty years that software is notoriously difficult to verify as correct. This lesson must be part of the evaluation of the security and reliability of electronic voting machines.

The proponents of proprietary data will argue that both hardware and software have undergone testing by an Independent Testing Authority (ITA). We clearly, however, cannot view as reliable the software testing done by the ITAs. They have [JONESB] certified software that later had to be patched, and they have certified software with the well-publicized back door supervisor passwords. We believe those who are knowledgeable about software are unimpressed by the certification of reliability by the ITAs. We would be much more impressed if the legions of graduate students around the world had tried and failed to do their worst against the ESS or any other electronic voting machine.

The argument that is made by the vendors is that intellectual property issues should trump the right of voters to trust the election process. We hold it to be self-evident that this argument must be rejected.

We note also that the adoption of a standard statewide machine, such as South Carolina is in the process of doing, makes an attack on the machine all the more likely. The vulnerabilities and threats will not have changed with the adoption of a statewide machine, but the risk will have increased enormously because the potential payoff has increased. With multiple voting machines from multiple vendors in use, a statewide attack would present almost insurmountable logistical problems to an adversary. With a single statewide machine, all the eggs are placed in one basket; it thus becomes vitally necessary that that basket be carefully guarded. Unfortunately, the state of South Carolina (and we suspect many other states) seems incapable of adequate guardianship of the system. Moreover, it seems unwilling to accept that guarding complicated computing equipment might well be different from guarding mechanical or optical devices.

The System and Its Security Must Be Simple

What is true in South Carolina is probably also true in many states: much of the process of conducting elections is done at the local, not the state, level. It is therefore almost guaranteed that the expertise we might have at a central state level will not exist at the local level. To ensure reliable elections, the system that is used must hence be simple enough that only a minimal competence is required. We do not make these observations with the intention of being condescending. Realistically, the funding exigencies that are

a constant problem for local governments will make it difficult for them to attract and maintain staff who are up-to-date on computer security issues and competent to maintain a complex system. Even if funding were not an issue, the sheer number of qualified staff that would be necessary statewide to manage a complex system is unlikely to be found.

We believe the case of South Carolina is typical. In discussions with the SCSEC, it was admitted that SCSEC has no competence whatsoever in computer security. They have no person on staff to maintain their own computer network, and they apparently rely completely on other state agencies to supply the computing necessary to tabulate votes. A private company had been contracted to handle some of the processing for the 2004 election. When the SCSEC was asked by the first author about the technical details of security of the ESS machines, the SCSEC was unable in-house to answer any questions. Instead, all questions were directed to the vendor. We consider all these details to be portents of serious danger, and we expect South Carolina is not unusual in this regard. We argue further that the use of proprietary hardware and software contributes to the complexity of the system. Not all the problems that are likely to occur in the use of the system will be covered in the training of election workers. With the relative infrequency of elections and the voluntary nature of many election workers, it seems unreasonable to expect them to become sufficiently fluent with a proprietary technology to be able to make informed (and quick) judgement calls in unanticipated situations.

The primary risk engendered by a complicated system is that it will not be implemented correctly on Election Day and thus disruption will occur. This has been one of the main

concerns and one of the main problems with electronic machines in the recent past, although perhaps not to the same extent on 2 November 2004 as in previous elections and primaries. However, if and when a single statewide system is adopted, the potential for disaster increases because the same common error in judgement would be applied statewide. Militating against this possibility, of course, is the fact that with a single system one need only train election officials in the use of that one system. If the expertise in computer security is minimal at the state level, however, it is difficult to see how expertise could be transmitted from the state to the local level.

Current Systems Are Unacceptable

Not surprisingly, we do not believe the ESS system being purchased for South Carolina meets the standards that voters have a right to expect. The methodology for providing security is deeply flawed, in that most of the alleged security provided is through proprietary IP; it is specifically taught in most (if not all) university computer security classes that this is a long-rejected principle of security [BRADLEY, FARKAS, JONESA, RABA]. The security that does exist seems weak and deeply flawed. According to the report prepared for the state of Ohio, the security of the supervisor PEB rests with three passwords, two of which are three characters long and the third of which is printed in the clear in the audit trail [OHIOA, p. 100ff]. With a supervisor PEB, the recorded votes can be cleared and the machine reset. This weak security is clearly unacceptable.

We argue also that the current ESS product is already regarded as flawed by its own vendor, and yet it is still be sold and used in elections, including the 2 November 2004 election. More than a year ago, at the time of the Ohio report [OHIOA, p. 95ff], the

recording of ballots in the ESS machine was done in the clear, with no bits added for encryption or authentication. At the time of the Ohio report, it was asserted that encryption/authentication was being added to the device, but as late as September 2004 such software had not been included in the machines sold to South Carolina [SCSEC]. We can therefore conclude that the 2004 election was conducted in South Carolina using voting machines whose security was known to be less than desirable. (The South Carolina contract apparently provides for upgrades to the new system if or when they appear, but it still seems unacceptable to be using the current system that is recognized to be deeply flawed in this respect.)

The current ESS system provides a modem connection on the printer. In South Carolina, for example, this is not used. This connection should clearly be physically disabled or removed completely. We mention this as an argument for simplicity. If the modem is present, it will be viewed as having a purpose, and it will be assumed to be reasonable to use it. Use of modem or internet connections will only be assumed to be a bad idea if it is clear, based on the device's capability, that such use is not possible.

Voters Should Be Able to Trust the System

This is the bottom line of a discussion of voting machines. It is destructive of the political process for voters to lose faith in that process. We point out, although it should be unnecessary, that the appearance of impropriety and corruption also colors the election process to a degree that damages voter confidence. It is entirely reasonable for voters to suspect corruption when, as in 2004, the leader of Diebold says he is "committed to

helping Ohio deliver its electoral votes to the president next year" [CBSA, CBSB, NEWSMESSENGER]. It is entirely reasonable for voters to fear foul play when journalists report that ESS has more than once installed uncertified software in voting machines [VOTERSUNITE]. It has been argued that public officials, by the nature of their status as public officials, should be held to a higher standard of conduct than ordinary citizens. By the same token, the vendors of voting machines should be held to a higher standard than that for more mundane companies. We dare not as a nation permit public officials to be viewed with cynicism to the point that it is not reasonable to expect fair conduct from them; we also dare not permit voters to lose faith in the election process by failing to provide proper scrutiny of the manufacturers of voting machines. This can be compared to the uproar over the Digital Encryption Standard and later of the Clipper chip, and then to the lack of complaint when NIST selected an algorithm as the Advanced Encryption Standard. Although those complaints were largely confined to the expert computing community, the lesson should not be lost on us. When the complaints against the technology become too strident, the only remedy is full and open disclosure. Under the current rules for certifying voting machines, the vendors are permitted to keep the system secret and the only testing that is done is conducted by companies paid for by the vendors. Those testing companies have a track record for not flagging fundamental software flaws, however, and the hardware has a track record of failure. Under these circumstances, the people have a right to know the details. It may not be possible to obtain absolute assurance that the election process is reliable, but a closed system whose trustworthiness is bought and paid for by private enterprises with a vested interest in the results is neither believable nor acceptable.

A Path Forward

In the realm of electronic voting, we have an unusual opportunity. These systems are nearly universally panned by all knowledgeable computer scientists (and doubtless have hackers anticipating their biggest and most rewarding "gift"). The authors of this paper suggest that vendors seek counsel from their harshest critics. If the adversarial relationship continues between the computing community that knows how to make secure and reliable systems and the vendors of electronic voting machines, the level of antipathy will only rise; litigation will persist, and the voters will suffer continued loss of confidence. Worse yet, the default seems at present to be the steady adoption of these machines, in part due to HAVA funding, so the security lapses will be widespread by the time decisions are finally reached in the litigation. What is at stake here is not just another bad product, a technology product whose time is not quite here, but a bad product that has the potential to seriously disrupt the fabric of our democracy.

Informational

This white paper is submitted in response to the call by the National Research Council for papers regarding electronic voting machines and the election process. Duncan Buell is a professor in and chair of the Department of Computer Science and Engineering at the University of South Carolina. He holds a doctoral degree in mathematics and has conducted research in computer security, high performance computing, computational number theory, and information storage and retrieval. Carter Bays is a distinguished

professor emeritus of the Department of Computer Science and Engineering at the

University of South Carolina. He holds a doctorate in computer science and retired in

2002 after a research career in computational mathematics and algorithm development.

The opinions expressed in this document are their own professional opinions; no claim is

made or should be inferred that these are the institutional opinions of their current or

former employers.

References

 [BRADLEY] "Ignorance is not bliss. Security through obscurity doesn't work. It only

means that the bad guys know things that you don't and will exploit your

ignorance to the fullest every opportunity they get." Tony Bradley,

netsecurity.about.com/cs/generalsecurity/aa/aa060103_2.htm.

[CBSA] www.cbsnews.com/stories/2004/11/11/opinion/main655162.shtml

[CBSB] http://www.cbsnews.com/stories/2004/10/22/politics/main650884.shtml

[FARKAS] Csilla Farkas, Lecture Notes 1, www.cse.sc.edu/~farkas/csce522-

2003/lectures.htm

[JONESA] Douglas W. Jones, "Auditing elections," *Communications of the ACM*, v. 47,

2004, pp. 46-51.

[JONESB] Douglas W. Jones, www.cs.uiowa.edu/~jones/voting.

[NEWSMESSENGER] http://www.thenews-

messenger.com/news/stories/20030828/localnews/150004.html

[OHIOA] Compuware Corporation, "Direct Recording Electronic (DRE) Security

Assessment Report," 21 November 2003. Available at

www.sos.state.oh.us/sos//hava/index.html.

[OHIOB] Compuware Corporation, "Ohio Secretary of State DRE Technical Security

Assessment," 2 December 2003. Available at

www.sos.state.oh.us/sos//hava/index.html.

[OHIOC] Nola M. Haug, "Maryland/Ohio Security Assessments Gap Analysis," 26

February 2004. Available at www.sos.state.oh.us/sos//hava/index.html.

[RABA] RABA Technologies, "Trusted Agent Report: Diebold AccuVote-TS Voting

System," 20 January 2004. Available at

www.raba.com/press/TA_Report_AccuVote.pdf.

[SCHNEIER] Bruce Schneier, "The nonsecurity of secrecy," Communications of the

ACM, v. 47, 2004, p. 120.

[SCSEC] Teleconference, 16 September 2004, with Ms Marci Andino and Ms Donna

Royson, SCSEC, and Mr. Ken Carbullido, ES&S.

[VOTERSUNITE] "ES & S in the news: A partial list of events,"

www.votersunite.org/info/ES&Sinthenews.pdf.

[WILLIAMS] Brit J. Williams and Merle S. King, "Implementing voting systems: The

Georgia Method," *Communications of the ACM*, v. 47, 2004, pp. 39-42.