N128W12795 Highland Road
Germantown, WI 53022
April 18, 2005

Janice Dunn, Office of the Election Commission
901 N. 9th Street, RM G-3
Milwaukee, WI 53233-1458

I am writing you to day as a member of the Wisconsin State Senate Special Committee on Election Law Review. I would like to propose 2 severable additions to Wisconsin State statute chapter 5.91.

Let me introduce myself and some background information.

My name is John Washburn and I am opposed to voting machinery which communicates electronically in any manner (internet or private network) with other devices. This opposition particularizes on the current, internet-enabled touch screen systems offered by Diebold, Sequoia and ES&S. While these DRE system do not currently meet the minimum certification requirements of 5.91(18), 5.91(11), or 5.91(1), they may (with sufficient and extensive modification) eventually be brought into conformance with Wisconsin state statutes.

To support my concern over network-enabled voting machinery I have included the following:

1. Two of the 4 items contained in petition to the Wisconsin State Elections Board as to why network-enabled machinery may already violate current state statute.
2. My short elaboration on the particular perils of internet-enabled voting machinery which was requested by the Executive Director of the WI SEB in preparation for my appearance before the borad on March 9, 2005.
3. An executive summary of the remote perverting of a Diebold touch screen DRE via the internet connectivity features of the AccuTouch system. The DRE tested was one which was actually used in the November 2, 2004 election.

The only benefit to the State of Wisconsin which electronic connectivity provides is the efficient and nearly, error-free transmission of election results from the voting machine to a central canvassing point. This would be helpful for example, for the City of Milwaukee to collect the results of 314, ward-level canvasses into a single municipal canvass. All other benefits of electronic connectivity are benefits to the vendor of the voting machinery, the programmer of the voting machinery or both. All of the benefits to the vendor and programmer come at the expense of the benefits to the clerk administering the election or to the trust worthiness of the results tallied by the machinery.

Fortunately, this single benefit to the clerks administering an election can be provided with out resorting to the dangerous and use of network connectivity. The election results can be burned to a CDROM drive or other medium which is read-only once created.

Other such media would be DVD-ROM, Programmable Read Only Memory (PROM) cards or, casting back 40 years to obsolete technology, punched paper tape. For the 2 serious examples (CD-ROM and DVD-ROM), the voting machinery can produce a paper report and also burn a CD-ROM with all of the election data in a simple data exchange format. These file formats include, but are not limited to,

- Tab-delimited files (Microsoft Excel and Lotus 123)
- Comma separated variable (CSV) (Microsoft Excel, Lotus 123, any SQL-based database)
- XBASE dbf file format. (Microsoft Excel, Lotus 123, any SQL-based database)
- Fixed column format.

Once the CD-ROM is burned by the voting machinery, the disk and all other election material is returned to the election clerk or commission. The data on the CD-ROM can be imported, compiled and collated in minutes. Once done, the data on the CD-ROM for a ward can be compared to the printed tape reports from that same ward. The CD-ROM approach has the added benefit that the CD-ROM can be stored, transported and reproduced without the risk of damage as is the case today with printed tapes.

I would like to propose the following 3 paragraphs be added to 5.91.

> ***(19)*** *It does not employ any mechanism by which the voting machinery can communicate with any device other than a single printer connected by a single cable not longer than 10 feet in length.*
>
> ***(20)*** *It shall not contain, produce or utilize any recording medium which can be written to more than once.*
>
> ***(21)*** *It shall provide a means such that any changes to the programming of the voting machinery, the internal configuration of the voting machinery or external configuration with locked boxes or other structures of the voting machinery can only be accomplished by the breaking of seals. Such seals and whether broken or not broken must be visible by casual inspection to any member of the public while the polls and canvass are open to the public.*

If the provision on seals for the voting machinery is added I would also add paragraphs to 7.51(2)(a) and 5.84 which read:

> **7.51(2)(a)** *Seals on voting machinery may only be broken by the chief inspector in the presence of at least 2 other poll inspectors and where at least one inspector of each the major parties described in 7.30 is witness to the breaking of said seals.*
>
> ***5.84(??)*** *Once the testing of the voting machinery is completed by the clerk, seals as will be applied by the clerk to the voting machinery in a manner which conforms to the requirements of 5.91(21) .*

Thank you for your time on this matter.

If you would like more information from me or for me appear before your committee, you may contact me at 262-238-8940. Beverly Harris has indicated she would be willing to appear before the sub-committee on the specifics of the security defects found to date in the internet-enabled AccuTouch systems from Diebold or regarding the significant problems internet-enabled voting machinery has caused around the country including King County, Washington, Alameda County, California, and Cobb County Georgia. She may be contacted at: 425-793-1030. Other persons the sub-committee may consider to invite on this topic include Douglas W. Jones of the University of Iowa and Jim March from Sacramento California. Professor Jones's work on this topic may be found at his website: http://www.cs.uiowa.edu/~jones/voting/. Mr. March work in California can be found at: http://www.equalccw.com/voteprar.html

In Liberty,

John Washburn

Do not certify touch screen voting systems from Sequoia, ESS or Diebold.

I urge the board to not certify any touch screen voting system from Diebold Election Systems (Diebold), Election Systems & Software (ESS) or Sequoia Voting Systems (Sequoia) for the following reasons

1) No touch screen voting systems of any of the vendors comply with Wisconsin statutory requirement 5.91(18) that the system produces a paper ballot which can be used later in a manual recounting.
2) Nor does system of any vendor conform to 5.91(15) which requires the elector be able to review this paper ballot ***prior*** to the casting of said ballot.
3) Systems from these vendors possibly also violate 5.91(1). Systems from these vendors require extensive manipulation by a poll worker to "set the ballot" for each elector. I have my doubts the required privacy of 5.91(1) can be maintained.
4) The Vendors cannot demonstrate any instance in any election where their machinery would have simultaneously met the Wisconsin requirements of 5.91(11), 5.35(4), 7.25, and 12.13(3)(f) had such election been conducted in Wisconsin.
   a) The possible exception would be if Vendor technicians present in polling places were designated as machine custodians under 7.25 by the appropriate clerk or commissioner. Then, the programming changes and system manipulations done in prior elections in other jurisdictions around the country by technicians employed by the vendors might possibly be permitted, since the clerk-designated machine custodian would be performing, recording and certifying said manipulations.
5) All of these Vendors prevent independent review of the software used in their touch screen systems. This violates the spirit if not the letter of testing requirements described in 5.84. Reviewable, open-sourced voting software is available. Therefore, until the Vendors source code is reviewed by a person or body selected by this Board, no systems from these vendors should be certified. Two of the foremost experts on software security are at the University of Wisconsin – Milwaukee; Doctors Davida and Yao. I would urge the Board to seek the counsel of these 2 men if such a system review is ever permitted by any of these vendors.
6) Diebold especially is not to be certified for these additional reasons.
   a) The software (GEMS) of Diebold contains 2 databases upon which election statistics are stored. Because of this conformance to 5.91(11) cannot be independently verified by a clerk or commissioner performing the testing described in 5.84. Which set of books is the clerk viewing?
   b) Since access to and manipulation of the data in the pair of Microsoft Access databases used by GEMS is unrestricted for any person with physical access to the voting machine, the statistics gathered and reported pursuant to 7.51 cannot be independent verified by the chief poll inspector the machine custodian or other poll inspectors.
   c) Diebold software implementation of cryptography uses a single, hard coded key for use by an ECB implementation of the antiquated 1977 cryptographic standard, the DES. Such manifest programming incompetence was discovered during a software review of some but not all source code to the GEMS system. This partial review was not authorized by Diebold. The results though do indicate a full software review is order before certification is granted.

I would urge this Board to
request and lobby the Legislature
to add an additional provision to 5.91

This provision would prohibit voting systems to have any communication equipment which permit the voting machine to communicate in any way with any other device except to exclusively communicate with printer located no more than 10 feet from the polling equipment.

1) Currently, both Diebold and Sequoia voting system have NIC cards which permit connection to the internet or any other IP device. Further, every Diebold and Sequoia touch screen system in every election to date (regardless of jurisdiction) has had, during the time the polling was open, a ***live*** connection to the internet. I concede having a piece of polling equipment communicating with other machines or accepting downloads for reprogramming (i.e. installing patches) is not expressly prohibited by state requirements. But, I believe such communication is bad election policy. The legislature should address this new vulnerability.
2) But, even in the absence of clear statutory requirements, this Board can reject the certification of such communication-enabled voting machinery on the grounds that such communication (potential or actual) either violates compliance with 5.91(11) or prevents auditing and verifying the said machines' compliance with 5.91(11).
3) The installation of any patches (potential or actual) is also grounds for this Board to bar communication-enabled voting machinery. The installation of any patches after the performance of the testing required by 5.84(1) would invalidate said testing. The statutes in 5.84 require all voting machines be tested prior to any use by an elector.
   a) Since all 3 vendors have in the past patched the software of its systems without the knowledge of the governing election officials, such concerns are warranted.
   b) Also, communication-enabled voting machinery limits the ability of the governing election official from even ***knowing*** if such software alterations have occurred. Without such knowledge the affected clerk or commissioner would be unaware that re-testing under 5.84 was required; let alone executed.
   c) None of the prior instances of "patching" done by technicians of these Vendors during past elections in other jurisdictions would have conformed to the requirements of 5.84.

Why No Internet Connection

Introduction

My name is John William Washburn. I reside at N128W12795 Highland Road, Germantown, WI 53022. I have been asked to elaborate on my concerns regarding internet accessible voting machines.

I have been a software developer from 1985 through 1994; first as a Fortran and Pascal programmer and then as a developer of Windows applications and device drivers. From 1994 to the present I have been working in the field of software quality assurance in several capacities. I have also held certifications from the Milwaukee-based ASQ. Software development continued as an avocation and because of this I have written Windows applications in every version from 1.03 to present version Windows XP. I am also fluent in C/C++, Java, Perl, ASP, Visual Basic as well as dozens of other obscure programming and scripting languages. During this time I have maintained an intense interest in computer security as well as software quality.

This should indicate I am not a technological Luddite. Still, when it comes to elections in the state of Wisconsin the system I would prefer is no voting machinery at all except for a good counting scale. Yes, I would like to see people count ballots at all polling places by hand. Aside from being cheaper than voting machines, I believe such a system with counting scales would be both more secure against fraud and more accurate. The counting scale should have a capacity of 5 to 10 Kg and a resolution between 0.1 and 0.2 grams. A counting scale would allow for permanent paper ballots, the ability to recount manually, and would reduce errors substantially. The ballot counting would be done by having the poll inspectors / local canvasser separate out the ballots by candidate and weigh the ballots on the counting scale. The display from the counting scale is the number of ballots on the scale. Tallying then proceeds as outlined in WI Statutes 7.51.

I am in a small minority in this opinion. But, the danger posed by voting machines which can communicate with other devices is significant. In my opinion what benefits exist are dwarfed by 2 possible dangers arising from testing and security. In both software quality and security: ***Complexity is vulnerability***. Any communication path makes software harder to test and harder to secure.

Testability

Communication limits the validity of the testing required under WI Statutes 5.84 on 3 points

1. Machine software must be "frozen" before an election and not altered until the canvasses (local, municipal, county and state) are completed
2. Change detection difficult
3. Non-certified software has been run

Frozen Code

Such communication capability is sold by device vendors as a positive. The NIC cards, WI-Fi cards, USB ports or disk drives (both floppy and hard) allow the software on the machine to be maintained more easily and more cheaply. I agree with both statements. I contend mutable software is an undesirable feature in voting equipment. After the testing performed by a clerk or commissioner, the software that was tested should be "frozen" and "static" until the election canvassing is complete. The more frozen and more static the software is the better. The goal of voting machinery design is not the convenience of the programmer or to reduce the costs borne by the vendor to create useable software. The goal for using voting machinery is to provide more reliable and more secure election results for the State of Wisconsin.

The current Scantron-like systems have the programming "burned" into an PROM (EPROM or EEPROM) located on a removable card within the machine or a PIC card inserted into the machine. In order to alter the programming of a machine, I need to open the housing of the machine, remove the card, remove the chip, replace the old chip with a new chip, and re-secure the machine housing. This assumes I can "burn" a replacement EPROM ahead of time which works correctly with no testing. With communicating voting machines I can upload the replacement code from a diskette, a USB flash drive, my palm pilot via the WiFi, or from my server via the IP address of the NIC card.

Every communications path (USB port, NIC card, WiFi port, disk drive) erodes the ability to freeze the code and prevent software upgrades.

Detecting Changes

This leads to the second point: communications paths (USB port, NIC card, WiFi port, disk drive) erodes the ability to know the software has been upgraded since the testing. Because of this the clerk may have no way of knowing if the code she/he tested is the same code in the machine on election day. If you do not know if the software has changed, how do you know if another test is in order?

Uncertified Software

The 2 prior points could be dismissed as the delusions of a voting machine rube. Unfortunately, the touch screens by all 3 major vendors (ESS, Diebold and Sequoia) have been found in other elections and other jurisdictions to be running software at version levels higher than the version which was certified and tested. For more details on these instances I would refer you to the volumous work of Beverly Harris, Jim March, the California Secretary of State in her committee's report on touch screens at http://www.ss.ca.gov/elections/taskforce_report_entire.pdf and the Qui Tam and Sacramento suits against Diebold in California.

For software quality: ***Complexity is vulnerability.***

Security

Voting machines with communication capabilities open up the possibility of a new ***KIND*** of vote fraud. Classic frauds of the past include: stealing ballot boxes in transit to counting locations, swapping ballot boxes while in transit to counting locations, stuffing ballot boxes, halter voting (Voto de Cabresto) and others. All require access to the voting equipment, the elector or both. Voting equipment which can communicate via IP, creates the possibility a single person from a remote location can manipulate the results of or the software on many machines. For example, I could remotely rearrange the order of candidate names stored in the executable code or stored on the database. Using the Wisconsin ordering from November 2, 2004 this creates the following changes.

John Kerry	to	Micheal Badnarik
George Bush	to	David Cobb
Micheal Badnarik	to	John Kerry
David Cobb	to	George Bush
Ralph Nader	to	Ralph Nader
Jim Harris	to	Jim Harris
Walter Brown	to	Walter Brown

The software will still record on the database

100 votes for election 1 candidate 1,
100 votes for election 1 candidate 2,
1 vote each for election 1 candidates 3 through 7.

The proposed name change takes up the exact same memory. Thus, this re-arrangement is feasible even in EPROM based programming, let alone an MS Access or SQL database. With IP access, a dozen or hundreds of such uploads are possible and can be done in minutes.

If done at the correct time, the results which print on the tape total would read:

100 votes for election 1 candidate 1 (Badnarik),
100 votes for election 1 candidate 2 (Cobb),
1 vote each for election 1 candidates 3 through 7: (Bush, Kerry, Nader, et. al.).

Absent any other indication other than your surprise at the will of the voters, these numbers must be accepted as correct according to 7.51(2)(h).

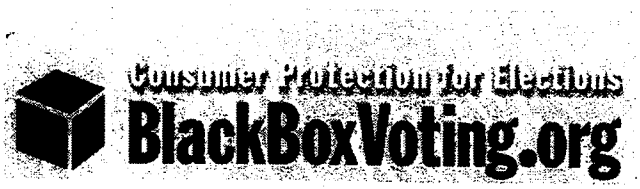
I concede this fraud is unlikely. But, currently it is only possible if I can corrupt the software "burned" into the PROM and the bogus software counts the first 25-75 ballots correctly in order to provide proper results during the 5.84 testing. Communicating voting machines add the possibilities of remote or real-time tampering to the threat matrix which must be considered.

Complexity is vulnerability. This is because complexity increases the attack surface of software. For security the goal is to minimize the attack surface. Communication paths increase the attack surface not minimize it.

So far I have spoken about malicious changes. There are risks posed by well-intentioned patches and changes. If the patch software is faulty, the machine may stop working. This is because complexity of a system determines the number of failure modes for a system. If you want robust systems, simple is preferred over complex.

Links:

http://www.newscientist.com/article.ns?id=dn4584
http://www.blackboxvoting.org/
http://www.serendipity.li/jsmill/bbv_050119.htm
http://avirubin.com/vote.pdf



To: John Washburn

Re: Investigations of election and voting systems

From: Bev Harris, Black Box Voting, Inc.

Date: April 13, 2005

Executive Summary: Real Life Hack of the Diebold Voting System

Black Box Voting is a nonpartisan, nonprofit 501c(3) consumer protection group for elections.

1) In mid-February, Black Box Voting, together with a computer security expert and professor of computer science, and an in-house videographer for Black Box Voting, along with a separate film crew for an independent documentary production, with the permission of local officials, proved that the Diebold system can be hacked.

This was not theoretical or a "potential" vulnerability. We hacked the vote on a real system in a real location using the actual setup used on Election Day, Nov. 2, 2004. We were allowed to try several different kinds of hacks. One, a remote access hack written up on Black Box Voting in Nov. 2004 based on information contained in the Diebold memos and on actual software, did **NOT** work. Another method, implanting a virus, **DID** work.

Using a simple virus-like script written in Visual Basic, a script unsophisticated enough that many high school students would be able to create it with just the Visual Basic lessons they get in low-level computer classes, we altered an election by 100,000 votes. This left no trace at all in the central tabulator program. It did not appear in any audit.

We did not need any special information in order to execute the virus. The only information needed was the name of the candidate and the amount (or percentage) of votes we wanted to change. The virus was so simple it could be sent in an e-mail, typed into the computer on "notepad," copied onto the computer by disk when transferring interim results, left on the computer by any Diebold technician or any in-house tech person, or put on the computer during repairs or upgrades.

2) In another real-world example, we obtained the actual file set used in the Nov. 2 election from a real election. In this situation, the local official did not know how to run her Diebold system, so a Diebold tech ran her election on Nov. 2. She remembered that his name was "Rob" but did not remember his last name. Rob went home after the election, and no one in the county was able to access their own voting system. They were distraught because they did not know how to provide our public records request. Therefore, we were given permission to sit down and copy the files. We found that we could easily hack the password in this real setting, and also that we could easily alter the audit log. We also discovered that the password for this real election, set up by Diebold,

was easy to guess: The password was "diebold" and there was little security on the tabulator. There were indications on the Windows event log for this system that at one point the computer was trying to "dial out." We do not know why or where the tabulator was trying to dial out to.

The significance of these two reports is this: By hacking into the central tabulator so easily, we showed that Diebold has not told the truth about the security of its system. Indeed, the software being used in BOTH examples was exactly the software found by Bev Harris on the Diebold site. That was not old software, or out of date, nor had it been fixed or flaws corrected. It was used in Nov. 2004 with security problems wide open.

We videotaped both reports. I have not provided the names of the officials, nor the locations, because Diebold has been aggressive about pursuing punitive action against officials who are brave enough to try to find out about their own systems.

We saw that there are several ways to compromise the system, and we are working on replicating the virus-like hack with other cooperative officials. The security expert we worked with says that no patch or "fix" Diebold can offer will correct the hack we performed, because its enabler is built into Windows and cannot be removed without obliterating the ability to use the central tabulator. In addition, we also have now identified other ways to manipulate the vote, and will be testing them as well.

Bev Harris
Executive Director
Black Box Voting, Inc.
206-335-7747 (cell)
425-793-1030 (office)