The Dangers of On-Screen and Online Electronic Ballot Marking

David Jefferson[1] & Candice Hoke[2]

To avoid the mail delays inherent in requesting and receiving a blank absentee ballot overseas and military voters have recently been permitted to download an electronic copy of a blank ballot via the Internet. While the transmission of blank ballots may be a reasonably safe operation, the best practices and security procedures for this option have never been clearly detailed. Of course no system should permit an electronic copy of a voted ballot to be *returned* to election officials via the Internet because of the great danger this poses to that voter's ballot and to the integrity of the entire election as a whole.[3] But on-screen ballot marking also poses very serious dangers to the privacy and integrity of elections even without electronic return of voted ballots. In this brief essay we explain the reasons.

Electronic marking of ballots introduces many privacy security holes

The most secure and private method for using an electronically downloaded blank ballot is for the voter to simply *print the blank ballot* along with a *blank* identification form (in some jurisdictions also containing an oath for the voter to sign). The voter should then fill in both of them *by hand, on paper, with a pen*, and mail them back to the home jurisdiction using conventional or military postal mail.

However, some vendors and election officials are implementing a modified ballot marking procedure that is similar, at least superficially, but that instead poses extraordinarily serious privacy and security threats. In this variation, the blank ballot is downloaded as before, but the voter fills it out *on the screen, electronically*, using the mouse and keyboard, *before printing it*. The voter then prints the filled-in ballot and mails that back to the home jurisdiction (with the signed ID form).

Voting system vendors suggest that electronic ballot marking does not present any security threat since the voted ballot is not transmitted over the Internet (implicitly recognizing that there *are* extreme security dangers in that). But in fact, the way most systems are implemented the votes in fact *are transmitted over the Internet to a server managed by the vendor so that the vendor can see and count the votes if it chooses!* Unfortunately, the seemingly small change from entering votes by hand to entering votes electronically introduces huge privacy holes that in our judgment greatly outweigh the comparatively minor advantages.

[1] Dr. David Jefferson, Lawrence Livermore National Laboratory, d_jefferson@yahoo.com

[2] Prof. Candice Hoke, Cleveland Marshall College of Law, shoke@me.com

[3] *See e.g.*, http://servesecurityreport.org/paper.pdf; and http://www.verifiedvoting.org/downloads/votingtransactions.pdf

How electronic ballot mark works

To understand the most severe dangers of electronic ballot marking, you first have to understand the difference between how it *should* work (if it must be done at all) and how it *does* work. It does not work the way you would probably expect.

The way it *should* work is this: The voter contacts the appropriate server through a web browser to download and display a blank ballot on screen. Then, still using the browser, the voter makes his vote choices on screen, electronically, with a mouse (in the case of a desktop computer) or a finger (in the case of a touchscreen phone or tablet) and clicks on a final button when finished. The browser (and other related software) then renders a finished voted ballot image *entirely within the voter's computer*, and prints that page for the voter to mail back to his local jurisdiction.

But that is not how it actually works. What really happens is that after the voter has finished making his vote choices electronically and clicks on the final button, *the voter's choices are then packaged and sent back to the server*. The server, not the voter's computer, produces the final voted ballot page image, and then sends that image back to the voter's computer where it is printed.

On screen marking software is part of a "voting system"

One point should be clarified up front: Any software used by a voter to help mark his ballot *is legally part of the "voting system."* The Help America Vote Act (HAVA) § 301, defines a voting system (permissibly used in federal elections) as "the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; to cast and count votes; to report or display election results; or to maintain and produce any audit trail information." Based on this language, the federal agency that certifies voting equipment, the U.S. Election Assistance Commission (EAC), ruled ballot marking devices to be part of a "voting system" when it certified the AutoMark as part of the ES&S Unity 3.2.1.0 voting system.[4]

Automated vote secrecy violation

When a voter fills out the ballot on screen, he or she is entering this information into a software application or browser that is connected to the Internet. The problem is that voters ordinarily have no way of knowing what that software, or other software on that computer, might do with their votes besides printing them. The voter is essentially using black box software, often proprietary, with no way of verifying exactly what it does. For example, the software used for marking ballots could silently send a copy of both the votes and voter ID data (such as the computer's unique IP address) to a third party as part of a broad, automated vote secrecy violation or coercion scheme. Or it could send the data to a candidate's or political party's server to offer "early returns" to help them tailor their late campaign messages, or to focus their final expenditures in a get-out-the-vote effort. The data might also be accumulated on

[4] *See* http://www.eac.gov/eac_certifies_ess_unity_3.2.1.0_voting_system

a server for targeted mischief of various kinds at a later time. Voters generally cannot know what happens to data they enter into Internet-connected software.

Even if the ballot marking software acts as expected, many employers take the position that employees should have no expectation of privacy when using the employer's computers and network infrastructure. Employers are within their rights to electronically spy on anyone voting using their computers.

The general secrecy of ballots is a vital systemic voting security issue. The secret ballot principle is by far the strongest protection we have against vote coercion, vote buying schemes, and unfair political advantage when one party has voter preference information not possessed by all. It is essential to protect this powerful democratic safeguard. Fortunately it can be protected in this case by the simple expediency having voters fill out their ballots by hand, on paper, instead of electronically.

Malicious ballot marking software

Automated privacy violation is the most obvious threat enabled by voters entering their votes electronically instead of by hand, but it is not the only threat. Malicious ballot marking software may selectively disenfranchise voters who do not vote the way the programmer wants. The software could, for example, be programmed to modify the ballot before printing it. The software could make a change in the printed copy that the voter is unlikely to notice but that makes it clear to officials or the scanning software that the ballot has been tampered with, perhaps by rearranging the order of the candidates' names or printing an improper barcode. Alternatively, the software could simply "crash" and fail to print a marked ballot containing votes that the programmer does not like.

It is important to understand that simply disconnecting from the Internet while marking the ballot on-screen cannot eliminate these risks. The software could easily store the votes for transmission later when the computer is reconnected, and the voter would likely never know. The real core of problem is entering votes into ballot marking software in the first place, and that is what should be avoided.

Unofficial ballot marking software

If online ballot marking software is permitted, it is likely that unofficial, alternative online ballot marking software may become available and marketed to voters openly. As a fanciful example, these could be integrated with Facebook^{TM} in a "share your vote" feature, or they could be in the form of alternate web sites offered by political parties or special interest groups to provide convenient ways for voters to mark a straight ticket even where state law does not offer that option on its other voting systems. Unfortunately, there is really no way to prevent such alternative software from being circulated by individuals or large organizations. Some might even argue that the introduction of an alternative ballot marking software option could be desirable. But just as with the official software there will be no way for a voter to know what the alternative ballot marking software really does, and whether it is honest or malicious. *The best practice is simply not to allow online ballot marking in the first place, but to insist that voters mark their ballots by hand.*

Barcodes in online ballot marking systems

Some online marking systems print the voter's ballot in the traditional form with filled-in ovals, but then add a bar code that is supposed to reflect the voter's choices in coded form. The idea is that when the ballot reaches the home jurisdiction, the barcode will be scanned rather than the human-readable ovals. Then election officials will use the information in the barcode to generate a copy of the voted ballot on official ballot stock so that the copies can be scanned using the existing systems. Alternatively, officials may enter the information from the scanned barcode directly into the vote tabulation without creating a ballot copy.

This bar code idea, well intentioned though it may be, introduces other risks to accuracy and security. Malicious (or simply buggy) software might print the human readable ballot correctly, but then print a barcode with it that contains different votes. An average voter will almost certainly lack the tools and motivation to check the bar code before mailing the ballot to the election office, so the votes transmitted in the barcode and ultimately counted could be different from those the voter intended—and the voter would be unaware. Even if the official ballot printing software works perfectly, alternative software distributed by others very well might be malicious and corrupt the barcode.

One problem with barcodes can arise if a voter prints the electronically marked ballot along with its barcode, but then decides to add additional votes by filling in more ovals on the printed copy by hand, with a pen. Voters who do not understand the bar code design or purpose (and that would be almost all of them) will think there is nothing wrong with this. But the new votes added by hand will not be reflected in the barcode, and thus will never be counted.

Both of the problems caused by barcodes can be managed if these original ballots mailed in by the voters are included in a risk limiting audit process[5] at the home jurisdiction, and if the auditing is based on hand comparison of the human readable marks on the original mailed-in ballot (*not* the barcode) with the votes recorded in the canvass. But currently, almost no jurisdictions require such audits.

Smart phones and other devices using a cellular carrier

If the voter uses a smart phone or mobile tablet to mark his ballot rather than a desktop or laptop computer then the risk to vote privacy is far greater. It has recently been revealed that several major telephone carriers routinely preload smart phones and tablets with monitoring software called CarrierIQ that has been characterized as essentially *spyware*. That software can record every touch, keystroke, button push, app launch, or other interaction with the device, and can surreptitiously upload all of that

[5] *See, e.g.*, Philip Stark and Mark Lindeman, *A Gentle Introduction to Risk-limiting Audits*, http://statistics.berkeley.edu/~stark/Preprints/gentle11.pdf;
Principles and Best Practices of Post-Election Audits, (Lindeman, Smith, Halvorson, Garland, Addona, McCrea, eds.) http://www.electionaudits.org/principles.html; focuses on risk-limiting audits at http://www.electionaudits.org/bp-risklimiting.

monitoring data to the carrier.[6] Although public outcry might chasten carriers from such a move, no laws prevent carriers from monitoring the voting process if they choose to do so.

CarrierIQ is an example of the dangers posed by third party software. Users can be completely unaware even of its presence, let alone its dangerous capabilities. The only thing a voter can do to fully protect herself from this threat is, once again, to never enter her votes into a mobile device in the first place.

Limitations of testing and certification

You might think that these problems would not occur because any official ballot marking software would be tested and certified before being used in an election. But even if the official ballot marking software were subject to testing and certification (as it should be), standards for acceptable privacy, accuracy, and security would be required first, but they have not been developed. In any case no such testing or certification process would apply to *alternative* ballot marking software that would purport to "work with" the official software. Alternative software could be totally malicious, and still not be subject to any publicly accountable testing process at all. Most voters will not understand the risks that hidden features in the technology can disenfranchise them.

Even if testing processes were perfect (which they are not and cannot be) there is no easy way for ordinary voters to verify that they are using the officially certified software. Voters can easily be tricked into using phony or alternative ballot marking software that appears to act like the real thing, but is really a malicious substitute.

Conclusion: Never enter votes into an Internet-connected device

The bottom line is simple. As a general security rule ***voters should never enter their votes into any Internet-connected computer or device because there is no way to be sure what the software on that device will do with the vote information***.

It may be reasonable to provide a ***very limited exception*** so that voters with certain disabilities that prevent them from marking a paper ballot might mark their ballots electronically, but only after full disclosure risks and with the commitment of election officials and the affected voters to cooperatively work on determining the best alternatives to using these extremely risky online procedures. For the vast majority of voters and for the safety of the election system as a whole, the only safe method for absentee voting is to ***print the blank ballot onto paper, mark vote choices by hand,*** and ***mail the paper ballot through the postal service***.

Instead of promoting electronic entry of votes, voting system designers and election officials should stick to the best practices outlined here. By educating the public about

[6] *See, e.g.*, http://en.wikipedia.org/wiki/Carrier_IQ; http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/

the ways some proposed new voting technologies actually undermine fundamental voting rights and the trustworthiness of election results instead of enhancing them, we can all help protect the electoral process.