



Secure Remote Voting for Overseas and Disabled Voters

by Aaron Contorer

Chief of Products and Partnerships

Everyone Counts, Inc.

January 2009

Election officials are now taking online electronic voting seriously. Computer and phone networks can be useful channels for remote voters including soldiers and civilians overseas (UOCAVA), disabled (HAVA), and others.

Are computers and phones more or less secure than paper? What about fax? Can email be relied upon? How about the web or the Internet itself?

In this paper we explore what can and cannot be done with online voting technologies.

Reliable and timely access to a blank ballot

As a recent report from the National Institute of Standards and Technology (NIST) explained, the easiest-to-solve portion of UOCAVA voting is simply delivering ballots to voters. Technologies as simple as email and fax can transmit a blank ballot quickly anywhere in the world.

However, *a ballot which cannot be successfully voted and returned and counted is no better than no ballot at all.* Thus, the rest of this paper explores the rest of the problem.

Safe and reliable return of ballots

As the NIST report said, "election officials must be able to ascertain that an electronically returned voted ballot has come from a registered voter and that it has not been changed in transit. Because of this and other security-related issues, the threats to the return of voted ballots by email and Web are difficult to overcome."

Do you bank online? And is any money still in your account? Despite unlimited motivation to break into these systems, criminals are unable to penetrate online banking systems and drain the money. So we know that Internet services purpose-built for security can work well.

Does your bank let you withdraw money by email? Banks know that email is not secure. By the mid 1990s computer experts knew that in mere seconds an email can be made to appear "from" any person and any organization, regardless of its true origin. Better email software has been invented, but the system most Internet users use today is no more secure than it was in 1990. Furthermore, most email systems provide no privacy from the eyes of the sender's computer system administrator. Until we replace or reconfigure voters' email software worldwide, email is clearly not the answer to returning secret ballots securely.

Would you send a legal document by fax? You certainly can, and it works, and it's legal. Would you send a *secret* legal document by fax? Only if you are a very trusting individual. Voting rights advocates are furious about cases where citizens are required to vote by fax: this often involves completely sacrificing their right to a secret ballot. Faxes can be read on a phone line, and they often sit in plain sight at the receiving station. Making an altering or invalidating mark on a faxed ballot requires only a pen. And far from anonymous, faxes are automatically marked with their location of origin (whether accurate or faked). Fax is a handy technology, but utterly unsuitable for the return of secret ballots.

How does the military convey critical, time-sensitive, secret information? The answer is *digital encryption*. Extremely complicated mathematical formulas scramble the message with long numeric passwords or *keys*, yielding a series of numbers that read as nonsense to anyone lacking the secret decoding passwords.

Our company currently uses a military-grade system with an ever-changing 168-digit binary key, to encrypt each completed ballot before sending it to the tabulation office. Computers pick a new secret key for each ballot. Even a spy using a giant supercomputer could not hope to decode a single boxful of these ballots.

Encryption protects privacy but also prevents alteration: any change to the stream of numbers results in only gibberish when decoded.

Preventing invalidation

As we work to protect the rights of overseas and disabled voters, preventing the accidental invalidation of their ballots is crucial. We have all seen overseas military personnel going to great effort to vote, only to find their ballots discarded due to extraneous marks, overvoting, or the failure to fill out a signature block in the required format. Voters with disabilities have sent in many ballots whose intents were clear, but that were invalidated due to technical mistakes or extraneous marks.

Fax doesn't help, nor does email – even paper and a postage stamp do nothing to prevent accidental invalidation. Online voting, with real-time error checking before final submission, helps protect voters' right to be counted.

Assistive devices

Many blind, motor-impaired, or otherwise disabled persons have a computer or telephone which has been adapted to suit their needs. Online voting, by working with these adaptive devices, allows disabled voters to vote from home without the loss of privacy implied by manual assistance.

The secure audit trail

Auditors must ensure the proper custody and treatment of each ballot, from the moment it was cast until the count is complete.

The most auditable systems are the fully-online systems, in which each ballot can be tagged with an anonymous tracking number if desired.

The least auditable system is email. The Internet's system for routing emails was never designed to be auditable, and it is impossible to verify the path taken by an ordinary email between the sender's PC and the receiving machine. The email may go through any number of "server" computers in between – and as most are totally unencrypted, any server has the power to change or add to the contents. It is *routine* for servers to add to or alter emails, such as by adding routing information or noting whether the content looks suspicious. Many even discard emails without notice, as a defense from spam. Today's worldwide email infrastructure can be neither trusted nor audited.

Similarly, faxes may be electronically relayed and may be edited by the relayer manually or automatically. This is only common in large organizations, which use "e-fax" rather than "direct-dial fax" systems. The final receiver has no way to determine

the number of relays or edits a fax has been through, due to the lack of encryption.

Preventing “mystery software”

Mechanical balloting and mechanical tabulation introduced the “black box” problem: what is really happening inside that machine? Tests are routinely administered to detect defects and fraud attempts, yet tales of machine-assisted election tampering go back many years.

While even the simplest voting machine is subject to tampering, doubts grow dramatically when the machine contains parts – such as secret software – that election officials are *not allowed to see*. Computer experts agree this constitutes a serious risk – we must know what the machine is doing with the ballots, that they are being recorded and tabulated accurately and honestly.

The solution is *open code*. The technical workings of any device that handles votes should be fully open for inspection by officials. Software that is available to inspect is called *open code*. Open doesn’t imply “free to copy” – seeing my blueprints doesn’t license you to build my device. Many software experts believe that any voting computer should – or must – use open code.

Proof of receipt

Computers can effortlessly index vast amounts of information. Secure tabulation computers can let voters look up their ballots long after election day is over. Days after the election, a voter can visit a web site, enter his or her receipt number, and see a secret word or phrase he chose as proof that his ballot arrived safely.

This feature is one example of the power of technology to increase voter access and trust to levels impossible with paper ballots. In coming years we will see more such innovations throughout the voting systems industry.

Immunity from tampering

A well-designed trusted service can use other less-trusted technologies without danger. For example, paper ballots can be delivered using ordinary mail, not special “voter mail,” because the security is provided by special envelopes, ballot boxes, and careful handling procedures. Similarly, online voting systems can use ordinary Internet technologies to move information around the globe, as long as the voting systems add proper security to what’s already there.

The Internet equivalent of an envelope is encryption. When a message is encrypted, just like a paper inside a safety envelope, it cannot be read or altered along the way. Voting software using military-grade encryption can safely deliver ballots across any kind of Internet connection with no risk of spying or tampering. The better the voting software, the safer the ballot, regardless of how poor the voter’s Internet connection may be.

What about *paper*?

None of us would demonstrably and routinely *obstruct* participation in elections. Yet that is just what voting by paper does, especially when the voter is overseas.

The Australian Electoral Commission state that when they provided the option for overseas soldiers to vote online, the number who were able to vote on time and be counted rose from 22 percent to 75 percent.

And as reported in the *National Journal*, when the US Democratic Party allowed expatriates in the recent Presidential primary to vote abroad, voter registration increased tenfold, and 54% chose to vote online (vs. only 3% for paper mail and fax combined).

Many completed ballots arrive late or never, and many will be invalidated – and the great majority will never exist at all, because soldiers and other expats are simply too busy to deal with balloting by mail.

Paper gets a failing grade for ease of access (wait for it to come in the mail), security (a dishonest postal official can read or even alter your ballot), reliability (foreign postal services are notorious for delaying and losing mail), and access for the blind and motor-impaired. There is no encryption of the contents, nor timely verification of delivery.

If paper were not a familiar old technology, we would never seriously propose using it today. While we all like paper, its obviousness and its tangibility, modern online technology is more secure, accessible, timely, reliable, and usable.

Continuity of Service

One of the risks with any technology is that it will break. This gets worse when someone is motivated to break it on purpose.

Polling stations are subject to any number of obstructionist techniques. However illegal, we all know that these happen. Similarly, those with criminal intent may interfere with the mail. And absentee ballots can be mishandled by relatives or volunteers claiming to help.

Electronic technologies are not immune from these sorts of shenanigans. Malicious individuals seeking to interfere with an election can attempt to jam up phone lines, fax lines, or Internet connections, or to somehow cause a malfunction of the receiving phone system, fax system, or computer system.

Fortunately technologists have many years of experience protecting technical infrastructure from such threats. Large corporations routinely receive threats from criminals hoping to extort money from them; yet the web sites continue to run, telephones continue to be answered, merchandise continues to be shipped, and bank accounts continue to reflect the deposits made.

Every election technology will always be subject to malicious behavior from the enemies of democracy, or from sore losers who don't expect to win the day's election. We must be ever vigilant against such attacks. Technology does not make human nature better or worse, but it does provide us with tools and well-tested techniques for security.

Protecting voters from misdirection

Lately we have heard about fake or incorrect registration information sent to voters in the mail. The citizen who thinks he has registered but has not, or who thinks he has cast a ballot but has not, has effectively been cut out of the election.

Every channel has some "point of entry" where the voter shows up ready to vote, and must not be fooled by cheaters. While it is hard to secretly build a fake polling place, or to somehow answer a voting phone number that you don't own, it is relatively easy to print a fake paper absentee ballot.

Somewhere in between these two is the difficulty of building a fake web site. Fortunately there are techniques for a website to prove its authenticity. These can be as simple as telling each voter a personal secret number which the website must present, or as sophisticated as using an encrypted digital signature to prove the website's identity.

Overall we should consider telephone voting the hardest nut to crack for would-be fake pollsters; computer voting is also challenging; and paper voting is probably the easiest. Since we currently use paper for almost all absentee voting, this problem will get better through the use of technology.

Conclusions

Remote and disabled citizens must have their constitutionally mandated right to vote. Today's solution, paper, is failing miserably on timeliness, usability, and reliability – and it shows in the low numbers of military and overseas citizens who get their votes counted, and the great dissatisfaction of disabled advocacy groups. Technology can

be used to solve many or even all of these problems – but it must be the right technology. Email is a totally unacceptable solution, and fax has numerous limitations. Online (computer and phone) systems have the most potential to serve remote and disabled users, as seen in use by banks and the military, when designed and used correctly to deliver on their security promises.

□□☑

About the Author

Aaron Contorer is Chief of Products and Partnerships at Everyone Counts, Inc., which provides accessible, transparent, and verifiably secure multi-channel election services.

Mr. Contorer is a former executive of Microsoft, where he served as Bill Gates' technology advisor, and as architect for the transition of MSN onto the Internet. He is an inventor on over a dozen patents in computer security and networking.

See summary table on next page.

Appendix: Technical Approaches to UOCAVA Access

Scale: None – Poor – Fair – Good – Excellent

<i>Requirement</i>	<i>Paper</i>	<i>Email</i>	<i>Fax</i>	<i>Online Phone</i>	<i>Online PC</i>
<i>Deliver Blank Ballot</i>	Slow	Fast	Fast	Instant	Instant
<i>Prevent Invalidation</i>	None	None to Fair	None	Excellent	Excellent
<i>Privacy</i>	Good (if not disabled)	Poor - Fair	Poor	Good - Excellent	Excellent
<i>Prevent Alteration</i>	Fair	Poor	Poor to Fair	Excellent	Excellent
<i>Access for Blind</i>	None - Poor	Good	None - Poor	Excellent	Good
<i>Access for Motor Impaired</i>	Poor	Good	Poor	Excellent	Good
<i>Audit</i>	Good - Excellent	Poor	Poor to Good	Excellent	Excellent
<i>Evidence of Receipt</i>	None	Fair	Good	Excellent	Excellent
<i>Black Box Solved</i>	Excellent	Poor	Good	Excellent	Excellent
<i>Prevent Denial of Service</i>	Good	Good	Good	Good	Good
<i>Prevent Misdirection</i>	Poor	Fair	Fair	Good	Good