Issue Brief: Internet Voting and Uniformed and Overseas Citizens Absentee Voters

U.S. Public Policy Council of the Association for Computing Machinery

Executive Summary

The reforms introduced by the Military and Overseas Voter Empowerment (MOVE) Act embody the appropriate use of technology. While the MOVE Act is not a panacea, it offers solutions to many of the pressing challenges facing Uniformed and Overseas Citizens Absentee Voters (UOCAVA) voters, and its operational provisions are within reach at a reasonable resource investment. We also support the paper based kiosk model, which we discuss below, for remote voting.

The MOVE Act

Prior to MOVE, an overseas civilian or uniformed service person (UOCAVA voter) was dependent on the postal service to request a registration form, return the registration form, receive a blank ballot, and return the voted ballot. Mail could take a long time to travel between countries. Further delays resulted if a uniformed service voter's location changed during the process, which is common for military members. Consequently, voted ballots of UOCAVA voters often arrived too late to be counted.

Much of the motivation for the MOVE Act, which was signed into law in October 2009, was to address the problems of military voters. Reforms introduced by MOVE include:

- allowing UOCAVA voters to request and receive voter registration and absentee ballot applications electronically;
- requiring states to make blank ballots available electronically at least 45 days prior to any Federal election;
- requiring states to make Federal Write-In Absentee Ballots available online;
- providing for free expedited mail service for voted ballots of overseas uniformed service voters;
- forbidding notarization requirements; and,
- providing UOCAVA voters with the ability to track their ballots.

These reforms dramatically reduce the time required for the entire voting process, while increasing the time available for voters to cast their ballots.

Although MOVE allows for the establishment of one or more pilot programs “to test the feasibility of new election technology,” pilot programs are not mandated by MOVE. In particular, MOVE does not require any pilot program that allows internet or fax voting.

What is Internet Voting?

By internet voting, we mean returning an electronic form of a voted ballot over the internet using email, a web application, or an internet-based fax or phone (e.g. the iPhone). Internet voting can be done from a personal PC, iPhone, cybercafe, library, or kiosk containing a computer dedicated to voting. Kiosk voting can be unsupervised or supervised by authorized personnel; it can be paperless, or it can generate a paper ballot or record that is sent to a local election official. We refer to kiosk voting as dedicated voting; all other forms of internet voting are undedicated.

A major challenge of internet voting (and of any form of electronic voting) is that there is no known way to confidently audit electronic voted ballots, including ballots generated by email, fax, or phone voting. This is because of a fundamental difference between voting and commerce. While fraudulent transactions occur in commerce, we eventually detect them, because commercial transactions create records that are checked by the people who are allegedly the originators of the transactions. Election theft is much harder to detect, because there is only one transaction per person, and that person has no way to later audit his or her vote.

If no reliable post-election audit or recount is conducted, then incorrect software or malicious code could result in the wrong candidate being declared the winner.

One way to provide both the flexibility of electronic voted ballot delivery and the security and confidence that audits provide is to deliver the voted ballot electronically when it is cast and to capture the ballot in a paper form. This process is used by optical scan voting system where a voter marks a paper ballot and scans it into a precinct count optical scanner.

Unfortunately, it is not possible to duplicate this process for most internet voting. Home-based internet voting could create a paper ballot that could be mailed in, but a post-election audit or recount of an internet-based election would require that all internet voters mail in their paper ballots – an almost impossible condition.

Security Risks of Undedicated Internet Voting

Cybersecurity threats make all forms of undedicated internet voting insecure and vulnerable to election theft.

According to a December 2009 report from the Computer Security Institute, a survey of 443 companies and government agencies found that 64% had reported malware infections (malicious software such as viruses or worms) in the preceding year.

The Zeus virus, which steals money from on-line financial accounts, is an especially pernicious example. Because Zeus can simulate the victim's financial statement, the victim will learn of the theft only when some financial transaction cannot be finalized because of insufficient funds. A Zeus-like virus could be created that would steal a person's vote, instead of his money.

Zeus is hardly unique. The Conficker worm has the capability of “calling home” for more instructions. In other words, a Conficker-like virus or worm could remain quiescent until around Election Day, at which time it could call home to find out how its master wants it to vote. If a voter's computer is infected with malware that does nothing most of the time, there is a good chance that the voter will not know that the computer is infected. And even if he is suspicious, detecting and removing malware can be challenging, especially for a non-expert.

Election stealing software on a voter's computer can cast a ballot independent of the voter's intention, and the voter will never know. The computer screen will accurately reflect the voter's choice, but the malware can modify the voter's vote before it is sent over the internet. In other words, it is the malware that votes, not the voter.

Even the companies that produce internet voting software or process internet-based votes are not safe. News reports of government and corporate sites being hacked are becoming more frequent. In a March 2010 talk, FBI Director Robert Mueller is quoted as saying that the FBI’s computer network had been penetrated and that the attackers had “corrupted data.” The same article discussed the recent successful Google attack, which targeted Google intellectual property, as well as Gmail accounts of Chinese human rights activists:

> “Researchers investigating the Google attack -- thought to have affected at least 100 companies including Intel, Adobe and Symantec -- say that prime targets of the hackers were the source code management systems used by software developers to build code.”

The implication of Mueller’s comments and the Google attack is that voting system software could be rigged by outsiders, including attackers from another country. (The Google attack appears to have originated in China). Another disturbing aspect of the attack targets is that Symantec, one of the targeted companies, is a major supplier of anti-virus and anti-spyware software. The attacked companies, which employ large numbers of computer security experts, have vastly more resources than the relatively small internet voting vendors.

While external risks from hackers is significant, insider risks should not be ignored. As demonstrated by rogue trader Jerome Kerviel, charged with losing about $7 billion in unauthorized transactions at Société Générale by exploiting his insider status, a malicious trusted insider can be a major threat. Such an insider could hide election-stealing software in large software programs used by vendors and web- based voting sites. If the malware were cleverly hidden, detection could be very difficult.

Other risks of undedicated internet voting include spoofing (creating a fake voting website that looks very much like the real one), phishing (phony email that looks legitimate and attempts to trick the voter into going to an election-rigging website), denial of service attacks, coercion, and vote buying/selling.

The kiosk model has a dedicated computer connected via the internet (presumably using a secure network connection) to a central computer. The computer sends the voted ballot over the network.

Risks of Paperless Kiosk Voting

Paperless kiosk voting has many of the same risks as undedicated internet voting. These include malware infections, denial of service attacks, coercion, and threats to the voter's privacy that jeopardize his right to a secret ballot. While the risks of phishing attacks and vote selling are significantly reduced by the use of a kiosk, the accuracy and security threats, including the possibility that an insider might rig the machine, make paperless kiosk voting unacceptable.

Paper-Based Kiosk Voting.

There are a few forms of paper-based kiosk voting. In one, the voter makes his choices on a dedicated computer that prints out a voted ballot that the voter can verify. If the voter determines that the paper version is not accurate, then both the paper and the electronic versions are voided, and the voter votes again. If the paper version is accurate, then the electronic ballot is cast and the paper ballot is deposited in a ballot box and, together with the other ballots, transported back to the U.S. and ultimately to the appropriate local election official. Even if the computer deployed in the kiosk has incorrect or election-stealing software, the voter can check that the paper ballot or record correctly represents his vote.

Simply generating paper records provides no assurance that it matches the electronic record to which it should correspond; a statistically meaningful audit should be performed to verify the electronic record. If a significant discrepancy is noted, choices are to use the paper record as definitive, use the electronic record as definitive, or

discard the results. Based on our prior analyses, the paper record will provide a more accurate result in most cases.

Alternatively, the kiosk printer can print the appropriate blank ballot, which is then hand-marked by the voter. As above, the ballot will be deposited in a ballot box and transported back to the U.S., where it will be available for audit or recount.

Regardless of how the paper ballots are produced, any pilot program must address chain of custody issues to guarantee that the ballots are securely and promptly transported back to the U.S. in time to be properly tabulated.

There is a risk of vote-buying or coercion in an unsupervised kiosk or a kiosk with supervisors from only one party. Traditional election procedures manage this risk by ensuring that polling places have at least two supervisors with adversarial relationships (such as members of different political parties). Human supervisors are more trustworthy than an unattended computer for authenticating the voter.

Conclusion

We support both the aggressive pursuit of MOVE provisions for internet delivery of election materials to voters and the rapid return of voted ballots, so that they will be counted and available for post-election audits and possible recounts. We also recommend that if internet voting pilots are to be deployed, they should be limited to supervised, dedicated, paper-based systems, coupled with a statistically meaningful audit that should be performed to verify the electronic record.

While returning voted ballots over the internet could improve access and responsiveness for UOCAVA voters, internet voting introduces dangerous risks that can allow elections to be undetectably altered by malicious attacks or buggy software. Without paper ballots, it is impossible to conduct a post-election audit or recount of the internet votes.

Elections are a fundamental component of our national security, and they must be treated as such. Introducing new voting methodologies into real elections demands rigorous risk assessment to ensure the most fundamental election property: integrity.

Association for Computing Machinery (ACM)

With over 90,000 members worldwide, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting computing

educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

About the ACM U.S. Public Policy Council

The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's involvement with U.S. government organizations, the computing community and the U.S. public in all matters of U.S. public policy related to information technology. Supported by ACM's Washington, D.C., Office of Public Policy, USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities. USACM also identifies potentially significant technical and public policy issues and brings them to the attention of ACM and the community. USACM publishes a monthly newsletter, the ACM Washington Update, which reports on activities in Washington that may be of interest to those in the computing and information policy communities, and highlights USACM's involvement in many of these issues. USACM is actively engaged in number of public policy issues of critical importance to the computing community.

For more information about USACM, please contact the ACM Office of Public Policy at (202) 659-9711 or see http://www.acm.org/usacm/.