Comments on UOCAVA Remote Voting Systems

Arthur M. Keller*
University of California, Santa Cruz
Technology and Information Management
Baskin School of Engineering

Abstract

Ballots should be cast in secret, and counted in public. The gold standard is identified and authenticated voters who cast a paper ballot in a sealed physical ballot box, which is then shaken and opened at the close of polls, where the ballots are then counted using the sort and stack method in full view of observers. Remote domestic voting involves compromises to this gold standard. Remote UOCAVA (Uniformed and Overseas Citizens Absentee Voting Act) voting may involve further compromises to this gold standard. We consider measures to maintain the secrecy of the cast ballot, and allow for counting of the ballot in public.

1. Voting at the Polls

A voter in a physical polling place goes through three steps: authentication, making choices on a ballot, and casting that ballot.

Each voter in a physical polling place must be authenticated prior to casting a ballot. Part of this process involves the voter signing the voter rolls.

Once the voter is authenticated, the voter is given a ballot of the appropriate ballot style (jurisdiction and party) on which to make choices. The ballot may be given as a physical document to the voter, or a token specifying the ballot style may be given to the voter, with the token used to enable an electronic device to present the ballot to the voter. For example, the token may be an activator card for a direct recording electronic (DRE) voting machine.

The ballot must not contain any identification of the voter. Rather, the ballot is, for all practical purposes, anonymous of the voter.

Once the voter has made the selections on the ballot, the voter then casts the ballot. A physical ballot is cast by placing in a ballot box. There may be a scanner that notifies the voter if there are any overvotes, so the voter may correct the ballot or ask for a replacement. Overvotes became famous when some voters voted for both Gore and Buchanan on the infamous butterfly ballots in Palm Beach County, Florida during the 2000 election. On DRE voting machines, the cast vote record is recorded electronically, and there may be a paper trail for the voter verification of the ballot as well as to support auditing.

2. Domestic Vote-by-Mail Ballots

An increasing number of voters both receive and cast their ballots by mail. Each voter receives a paper ballot in the mail along with a return envelope. The voter marks the ballot with the voter's choices and seals the ballot inside the return envelope. The return envelope contains the information needed to identify and authenticate the voter.

The return envelope is often preprinted with the voter's identification, to facilitate matching the envelope with the voter record upon the ballot's return. However, the voter may be able to obtain a replacement envelope that has not been preprinted in which to return the ballot.

In some jurisdictions, the physical ballot serves as one token to indicate that the voter may cast a ballot. For example, in Santa Clara County, California, where the author has

* The author may be reached at ark@soe.ucsc.edu. This document represents his personal position, and not that of the IEEE Standards Working Group on Voting Systems Electronic Data Interchange, where the author is chair.

served as a Field Inspector supervising eight Precinct Inspectors, a voter who has been issued vote-by-mail ballot may surrender that ballot at the polls, and then cast an ordinary in-precinct ballot. In this case, there is a preprinted notation on the voter roll that indicates that the subject voter has been issued a vote-by-mail ballot, and a poll worker crosses out that notation when the voter surrenders the vote-by-mail ballot.

When a vote-by-mail ballot is received by the local elections official that supervises elections for the voter's residence, the identity of the voter is checked against the voter roll, and then the signature on the ballot is checked against the voter roll. Vote-by-mail envelopes are separated into the ballots that are to be counted and the ballots that are not to be counted. Vote-by-mail ballot envelopes should not be opened unless and until it is decided that the ballot inside the sealed envelope is to be counted.

While each state has its own rules and regulations, under California law, vote-by-mail ballots may be counted up to seven days prior to Election Day. During this period, the envelopes in the pile of ballots to be counted are opened and the ballots are removed. Voters trust the local election officials not to look at the choices the voter has made when removing the ballot from envelope, as this is the weak link in the anonymity of the ballot. Automated equipment for opening envelopes and removing the ballots can help ensure the anonymity of the vote-by-mail ballot.

Ballots, once removed from the envelope, are then counted, often using a bulk optical scanner vote counter.

3. Provisional Ballots

A voter casts a provisional ballot when the poll workers are unable to verify that the voter who appears at a polling place is registered to vote at that precinct and has not previously voted in that election. The provisional ballot is somehow identified so that it is not counted unless and until it is determined that the ballot is to be counted.

The author designed a provisional ballot envelope used by the Registrar of Voters in Santa Clara County, California, where all information needed by election officials to determine whether the ballot is to be counted is contained on the outside of the envelope (along with the records of the voter rolls). The provisional ballot is sealed in the provisional ballot envelope while it is determined whether the ballot is to be counted. Provisional ballots are not examined for counting until all vote-by-mail ballots cast have been counted.

For example, if a voter has been issued a vote-by-mail ballot, but is unable to surrender that ballot to the poll worker, then the voter is to vote by provisional ballot. If local election officials determine that the voter has not cast a vote-by-mail ballot, then the provisional ballot is counted.

A voter who is not listed at the voter rolls may be directed to the polling place for the voter's residence address or may cast a provisional ballot. Once local election officials have determined that the provisional ballot is to be counted, the ballot style of the provisional ballot must be checked to ensure that it matches the jurisdiction in which the voter resides. If not, then the ballot is transcribed onto a blank ballot of the correct ballot style of the voter, although choices made that do not correspond to the voter's jurisdiction are not copied. In some jurisdictions, the original and replacement ballot are each marked with the same tracking number, for subsequent auditing, but that tracking number is not identified with the voter. (A similar process is followed for damaged ballots with central count optical scan.) To preserve the anonymity of the voter, the provisional ballot can be separated from the provisional ballot envelope and placed with an identification of the proper ballot style, so that the inspection of the provisional ballot is done without knowledge of the voter's identity.

4. Distribution of Ballots to UOCAVA Voters

Vote-by-mail ballots are typically distributed to voters approximately one month prior to Election Day. While the voter will usually receive a vote-by-mail ballot within three days anywhere in the US when sent by first class mail, sending ballots overseas can take considerably longer. The vote-by-mail ballot may be received too late to return to the jurisdiction where the ballot is counted. Unfortunately, it is not possible to send out the ballots earlier, because of deadlines for placing ballot measures on the ballot and for candidates to register to run for office. Hence it is desirable for uniformed and overseas citizens to obtain their ballots electronically, so that they can cast their ballots soon after ballots are released to domestic vote-by-mail voters.

In order for the voter to obtain a ballot electronically, the voter first has to identify the voter's jurisdiction and ballot style. Because ballot styles change from election to election, there may be a website to which the voter presents his or her residence address to some website that determines the voter's ballot style. Such a website could be maintained by the local election officials or it could be another website more centrally maintained (such as by each Secretary of State or by or for the Federal Voting Assistant Program). During primary elections when the ballot style must be of the correct party, matching the voter's name and address against the voter rolls can be used to identify the proper party. In some jurisdictions, some voters (such as those registered "decline to state") may crossover vote to another party's ballot, and this choice of party ballot should be offered to the voter.

Standardization of ballot definition files and their correspondence to election jurisdictions will enable more centrally maintained websites to electronically distribute ballots to unformed and overseas citizens.

To maintain voter anonymity, the identification of the voter must be separated from the process whereby the voter selects the choices on the ballot. One way of accomplishing that is to distribute electronically a blank ballot that is printed and then filled out by the voter. If the voter makes the ballot selections using a website, then anonymity is more problematic. It may seem to preserve anonymity to use one website to identify a ballot style, which is then passed via a ballot style code to a different website, on which the selections are made. However, we know that the techniques for tracking visitors across multiple purposes for targeting advertising could be used to track voters between the two seemingly separate websites. Audits are necessary to ensure that there is no improper communication between these two websites. If the voter makes the choices on a website, the website may be able to produce a ballot for printing that appears like the Federal Write-in Absentee Ballot containing the voter's choices.

Distribution of ballots through the web may be subject to denial of service attacks as well as other hacking attacks. For example, if the ballot definition files can be hacked, then some candidate might not be presented to the voter. Security measures are necessary to minimize these and other problems.

5. Return of Ballots from UOCAVA Voters

The simplest and most secure method to return ballots from UOCAVA voters is for a printed ballot to be returned to the Registrar of Voters corresponding to the voter's registration address along with identity and authentication of the voter, and for that ballot to be counted in the manner of a provisional ballot. Enabling local legislation may be needed for these ballots to be properly counted provisionally.

A "failsafe" method to create a remotely cast ballot is to use a Federal Write-in Absentee Ballot. The ballot is to be inserted into an internal Security Envelope, which is inserted

into the mailing envelope along with the Voter's Declaration/Affirmation, and returned to the local election official. Instead of the write-in ballot, a printed ballot electronically distributed could be in the form of the standard vote-by-mail ballot (but not using the same paper stock and/or security markings).

Some jurisdictions require absentee ballots to be received by the close of polls, while others allow overseas votes to arrive late if they were mailed on time. Since provisional ballots are counted after ordinary in-precinct and vote-by-mail ballots, a reasonable compromise is to allow the ballots to be counted if they are received sealed by a secure ballot receiver (such as an American embassy or the mail office of a military base). The ballots would then be postmarked with the date, time, and time zone received and then batch expedited to a ballot distribution point based in the US, from where each ballot would be forwarded to the corresponding local election official.

Some have suggested that remotely cast ballots should be electronically transmitted back to local election officials. Doing so would reduce the time it takes to return the ballot, and it may also address accessibility concerns. There are a number of problems with this approach. A detailed analysis by David Jefferson, Aviel Rubin, Barbara Simons, and David Wagner can be found at www.servesecurityreport.org. Such a system would necessarily be accessible overseas, and therefore could be subject to cyber-attacks from hackers based overseas. Russian organized criminal organizations break into American financial systems and steal millions of dollars. It appears that the Russian government tolerates these criminal organizations, perhaps so they can engage in cyber-attacks, such as Web War 1 against Estonia during 2007, in which the Russian government can plausibly deny participation by using proxies. The Chinese cyber-break-ins against Google targeted at overseas Chinese dissidents indicates that even the best security can be broken. Google was able to detect the break-in with its world-class security team. However, local election officials do not have world-class security teams, so it is likely that such election hacking will not be detected. Do we want to allow the possibility that the next President will be chosen by overseas hackers who have broken into our election systems?

6. Authentication of Ballot Envelopes from UOCAVA Voters

There is already a known process for local election officials to authenticate the identity of the voter as part of determining whether to count a provisional ballot. Returning the ballot to the local election official for authentication and counting is the most secure process for having the ballot counted properly. The process can maintain the anonymity of the ballot, as described above.

Some have proposed delegating the authentication to remote officials. For example, each military base could have a designated official who authenticates voters against each voter's military identification and affixes an affidavit of authentication to the ballot envelope. However, that does not ensure that the voter is registered to vote (unless the voter rolls are checked at that time) and has not voted more than once.

Even voting via a secured voting kiosk on a private network does not eliminate this problem unless the voter is identified using the local election official's voter rolls, which means remote access to these voter rolls. Remote access to voter rolls of many jurisdictions involves many technical and security problems. For example, unless there is a paper ballot returned to election officials, auditing is compromised as it relies only on electronic records.

7. Counting Ballots from UOCAVA Voters

If paper UOCAVA ballots are returned to local election officials for counting provisionally, larger election jurisdictions may want automated mechanisms for counting these ballots.

Consider the following architecture for counting these ballot. Once the local election official determines that the ballot is to be counted, the ballot style(s) corresponding to the voter are identified. (There may be multiple ballot styles for a primary election when crossover voting is allowed.) The ballot is removed from the ballot envelope and placed on a scanner into which the list of proper ballot styles is entered. The scanner then compares the ballot against the ballot definition files and creates a cast vote record for the ballot (removing any contest for which the voter should not make a selection). The cast vote record is then added to the voting system's database of ballots cast. In this case, the distribution of ballot definition files and cast vote records occurs within a closed local area network, thereby increasing security.

8. Conclusions

Remote voting systems for uniformed and overseas citizens require particular care to ensure that the voter is properly registered, casts the ballot of the correct style, and casts only one ballot that is counted, and that the system maintains the anonymity of the ballot, supports election audits, is secure, and is resilient to cyber-attacks, including denial of service attacks.

Standardization of voter jurisdiction information, ballot definition files, and cast vote records will be helpful in the creation of remote voting systems.

The author proposes reference architecture for experimentation and analysis comprising these components.

- Voter jurisdiction information and ballot definition files are distributed to one more repositories.
- A uniformed or overseas citizen goes to a website with access to the repository, provides sufficient information to identify the appropriate ballot style, and the visits another website with the ballot style identification code.
- The voter is presented choices using an interface similar to that of a direct recording electronic (DRE) voting machine. This system has been checked to ensure that it does not have access any personally identifying information of the voter other than the voter's ballot style. But instead of recording the ballot electronically, a printed ballot is produced in the format of a Federal Write-in Absentee Ballot using a font easy to OCR.
- The voter mails to the local election official the printed ballot inside a Security Envelope, which is placed in a mailing envelope along with the voter's declaration/affirmation.
- The local election official identifies and authenticates the voter in the manner of a provisional ballot. If the ballot is to be counted, it is removed from the Security Envelope, placed on a scanner along with the jurisdiction (and party if appropriate) of the voter, for matching against the voter's ballot selections. The scanner creates a cast vote record, which is then securely transmitted over a local area network to a server, where it is entered into the database of cast vote records.
- Election results are periodically exported from the database of cast vote records using immutable media (such as a CD-R, not a network) to a reporting system where the results can be displayed to the public via the web.

While this architecture requires care in implementation to ensure security, reliability, availability, and accessibility, it would demonstrate the potential for efficient and timely remote voting by uniformed and overseas voters, facilitated through standardized common data formats for voting system electronic data interchange.