Issues and recommendations for Making Elections More Secure

Barbara Simons, David Jefferson, Philip B. Stark

The easiest ways someone could hack our elections remotely are through internet voting, voter registration databases, and voting machines that do not generate a paper trail. Fortunately, there are some steps that can be taken to reduce these risks, but prompt action is required.

1. Casting votes online is not secure: Votes sent over the Internet can be fabricated, deleted, or undetectably altered.

There is consensus among computer security experts that Internet voting, which includes scanned voted ballots sent as email attachments or faxes, as well as web based voting, is fundamentally insecure. Moreover, there are no national standards for Internet voting; there is no required testing; and there is no federal oversight. Most election officials have little access to computer security expertise, if any. Consequently, they may believe false security claims made by vendors of Internet voting systems.

Perhaps someday it will be possible to vote securely and anonymously over the Internet, but not now. Nonetheless, Internet voting is allowed for all Alaskan citizens and in 31 states for overseas military and civilians. (See https://www.verifiedvoting.org/resources/internet-voting/). This relatively small group of voters is most at risk of disenfranchisement due to malfeasance or error. We know from the 2000 election that even a small number of votes can change the outcome of an election.

The only time an Internet voting vendor allowed outside experts to attempt to hack an Internet voting system was during a pre-election pilot just prior to the 2010 midterm election in Washington, DC. Within 36 hours a team from the University of Michigan had total control of the system. They could change all previously cast and incoming votes without detection. If the test had not been conducted, an insecure Internet voting system would have been used in the midterm election. A similar attack is possible against any Internet voting system that currently exists – or that could exist – without a major, unforeseen breakthrough in technology. It would not take a nation state to mount an attack.

Immediate steps that can reduce the threat: The DoD, Homeland Security, the FBI, other relevant government agencies, election officials, and party leaders should warn voters NOT to cast their ballots over the Internet. Election officials need to understand that sending voted ballots as email attachments is Internet voting, something that many people, including a number of election officials, don't realize.

Fortunately, the 2009 MOVE Act requires states to make ballots available electronically at least 45 days in advance of an election. An overseas voter can download the blank ballot, mark it manually, and mail it in via postal mail. MOVE provides free expedited mail service for voted ballots of overseas uniformed service voters. Consequently, voter disenfranchisement should not be an issue. The party should reach out to federal, state, and local officials to encourage them to inform overseas voters of the benefits of the MOVE Act as expeditiously as possible. The party should also engage in an educational campaign where appropriate.

2. Voter registration databases (VRDs) are at risk of being attacked.

A VRD could be attacked either by padding the VRD with the names of partisan non-voters or by selectively remove the names of voters. The padding risk is exacerbated when states ignore common sense security guidelines.[1]

An attack that selectively removes voters' names from the VRD would be recognized when the names of a large numbers of people claiming to be registered were not in the VRD. However, opportunities to repair the damage during the election would be limited, and many voters could be disenfranchised. The risk of a VRD hack is not theoretical. For example, a breach of the Illinois voter registration system was discovered in July. (See http://statescoop.com/illinois-voter-registration-system-shut-down-following-cyber-breach).

The hacking threats can be reduced by immediately recommending the following best practices to election officials and voters.

a) Backup systems. Make sure the contents of the VRDs are backed up *to offline media*. (Backing up to online media makes the backup copy just as vulnerable to cyberattack as the primary). Take full backups now (hoping that they are currently free of malware). Then take frequent full backups (not just incremental) between now and November. *Make sure that new backups do not overwrite previous ones***.** (If backups are overwritten, problems that develop in the primary and are not noticed immediately get transferred to the backup, at which point it is not possible to recover).

b. Encourage voters to verify that they are registered. There should be oversight of election officials to make sure that they provide procedures for correcting problems expeditiously.

c. Provide a paper copy of the local VRD at each polling place as protection against Election Day attacks or failures.

d. Provide provisional ballots as a fall-back option. Local supporters and attorneys can pressure election officials to provide a sufficient number of provisional ballots at polling places to allow everyone to vote if the VRD fails. Voters should be informed that if their names are not on the voting rolls, they should cast provisional ballots. Voters also should be instructed on how to make their provisional ballots count. States and election officials should be warned of the risk of attacks and pressured to train poll workers about provisional ballots. Pressure must also be applied to count provisional ballots cast by legitimate voters whose names were illegally deleted from the VRD.

[1] For example, in Maryland all voters may vote absentee and may request to have their blank ballot sent to them over the Internet. Voters then mail their hand marked ballots to the local board of elections. **There is no signature comparison** or other means of authentication upon receipt. Because anyone from anywhere could obtain a blank Maryland ballot over the Internet, blank ballot distribution in Maryland should be limited to UOCAVA and voters with disabilities.

The following best practices should be implemented as early as possible, but there may not be time to implement most of them before the election.

e. Mass deletions and insertions should not be allowed close to the election. Any such change should require oversight by at least two senior officials; whether or not that is possible, there should be a daily check to ascertain if any mass changes have occurred.

f. Map the network: Except for the simplest networks, it makes sense to use a commercial network mapping tool to map all of the routers, links, hosts and other devices on the network to determine whether any of the devices has a path (wired or wireless) to an Internet-facing router.

g. Physically disconnect from the Internet: If a device or host on the network to be isolated has a path to an Internet-facing router, then physically disconnect it. *Do not rely on software disconnection*.

h. Prefer wired over wireless networking: Wireless networks (WiFi and even Bluetooth) should be avoided on networks that are supposed to be isolated. Although they have nominal communications radii of only 300 and 30 feet respectively, devices with special antennas can listen to and interact with WiFi and Bluetooth over much longer distances, which can allow them to be attacked remotely.

i. Transfer data in and out of the isolated network using only clean media: No device that has ever been connected to a host connected to the Internet should ever be used in the isolated (airgapped) network. Data brought in or out of an isolated network should be transported only on read-only or write-once media, i.e. CD, DVD, BD, CD-R, DVD-R, or BD-R. No personally-owned laptops, mobile devices, or thumb drives should ever be connected to the isolated network, even briefly. Thumb drives are particularly dangerous because they are mistakenly thought of as passive memory devices, but they are actually small computers that themselves can be infected with malware. (Remember Stuxnet). Since they are totally unnecessary inside an isolated network, and it is way too easy and tempting to use them to transfer data back and forth between networks, the best practice is to ban thumb drives entirely.

j. Revise procedures so that they do not depend on services unavailable on isolated networks: There can be no email, web access, message service, teleconferencing service, VPN service, or network time service on a network isolated from the Internet. It is important to recognize that neither software updates nor file transfers can be done by direct downloading from online sources to an isolated network. Updated software and database updates should be physically carried to and from the isolated network on write-once media. A thumb drive is not a good choice because first it would have to be written on an Internet-connected device and then read by a device on the isolated network, which is unsafe.

k. Employees who are allowed to update the VRD should have access to only those fields that are directly part of their jobs. Audit logs should report all changes by user, time, and device. These logs should be examined daily.

l. Software should not be upgraded or modified without appropriate precautions; software changes should not be allowed close to the election.

Given that there are no standards, no oversight, and no central location tracking the different voter registration databases, the database risk is difficult to address so close to the election.
For more information about securing DREs, see
http://usacm.acm.org/evoting/details.cfm?type=Reports%2FWhite%20Papers&id=123&cat=14&E-Voting.

3. Some polling place machines are a major cause of long lines. Direct Recording Electronic machines (DREs), typically touch screens, contributed significantly to the 2012 long lines, because voters had to vote on the DREs which were breaking down. These machines are way past their use-by dates: much of the software, which dates from the late 1990s and early 2000s, is no longer being maintained; the hardware is also failing. No one uses a computer from the early 2000s, but we are voting on DREs run by ancient computers. Many election officials are being forced to cannibalize some DREs to keep others running, resulting in even fewer working DREs.

A partial solution. While it's too late to replace impossible-to-secure paperless DREs, a partial solution to the long lines problem is to provide back-up paper ballots to distribute whenever the lines get long. (It would be nice if the paper ballots were made available to any voter who didn't want to vote on a DRE). Given the late date, the party should immediately urge election officials to provide back-up paper ballots. In addition, poll worker training needs to be updated and voters informed that back-up paper ballots will be counted in the election.

4. Voting machine results can be changed by software bugs or malware. It is more difficult to attack polling place voting machines than to make internet-based attacks, but software bugs or malware could impact the outcome of the election. Regrettably, in some or all of their counties, sixteen states still use paperless DREs that cannot be recounted or audited. Several of these are large swing states, such as PA and VA. Five states use only paperless DREs: DE, LA, SC, GA, and NJ. Georgia, which appears to be in play, votes only on Diebold paperless DREs that we've long known how to hack.[2]

Researchers have demonstrated that simply by swapping the memory card in one DRE, an entire jurisdiction can be infected with malware that could alter votes. Voting system vendors often "patch" or "upgrade" voting system software, including the software in tabulation systems; such patches could be used to inject malware.

A short term approach for paperless DREs: Ground observers should have rapid access to technical experts who can provide advice if a machine starts behaving strangely, such as highlighting candidate A's name when the voter has selected candidate B. The experts may recommend that the machine immediately be taken out of service and kept in a secure location so

[2] See https://www.youtube.com/watch?v=OJOyz7_sk8I. The leader of the team that made the hacking video in 2006, which the team hoped would convince people to get rid of the DREs, is Princeton Prof. Ed Felten. Prof. Felten is currently on leave from Princeton as Deputy U.S. Chief Technology Officer at OSTP.

that a forensic examination can be conducted later. This is not a very satisfactory approach, but it's the best we can do.

The best long-term protection against software bugs or the hacking of voting and tabulation systems is to have a paper record of voters' choices, preferably voter-marked paper ballots, which are used to check the accuracy of the tally. Typically, voter-marked paper ballots are read by optical scanning machines that tabulate the results. Because of the paper ballots, these machines can be checked by audits and recounts. While many states have paper ballots that are tabulated by scanners, not all of these states take advantage of the paper ballots to check on the scanner results.[3]

Best post-election practices for voting machines. For jurisdictions that have a well-curated paper trail, *risk-limiting audits* provide high confidence that if any errors, bugs, malware, or hacking altered the electoral outcome, the outcome will be corrected.

Risk-limiting audits have been conducted in California, Colorado, and Ohio. They involve manually inspecting a random sample of ballots. The "risk" in a risk-limiting audit is the maximum chance that the audit will fail to correct an electoral outcome that is wrong. In most states that have a paper trail, a simple form of risk limiting audits called *ballot-polling audit* is possible and affordable. The challenge is the logistics of coordinating the audit at the state level. Such an audit requires:

1. A paper trail;
2. Evidence that the trail has been curated well enough (no ballot-box stuffing, no missing boxes of ballots, not more ballots than pollbook signatures, etc.);
3. A "ballot manifest" for each jurisdiction, specifying how the ballots are organized into batches within the jurisdiction;
4. A way to manage the logistics at the level of each state to draw a statewide sample of ballots, allocate the work to counties and local election officials, and get the results back;
5. Agreement on risk limits, procedures, etc.

The sample sizes required would be rather modest in most states. The median sample size with a risk-limit of 10% for 255 state-level presidential contests from 1992 – 2008 is 307 ballots per state per election.

Other immediate recommendations: Best practices include publishing precinct-level results tallied in the polling place, immediately and again from the central tabulator; reconciling pollbook signatures with the number of votes in each polling place; inspecting seals on equipment; and prohibiting unsupervised "overnights" of voting equipment. All significant discrepancies and all discrepancies in electronic results, no matter how small, should be transparently reported and investigated.

Finally, there needs to be a policy for what to do when provisional or back-up paper ballots run out. Would photocopies of blank ballots be accepted by election officials? If not, what can be

[3] In Virginia it may even be illegal to conduct a post-election ballot audit.

done to prevent voter disenfranchisement from long lines as election officials scramble to obtain more paper ballots? This is an important issue that needs to be addressed before Election Day.