Basic Security Requirements for Voting Systems

Wenke Lee, Ph.D.
Secure, Accessible & Fair Elections Commission

October 8, 2018

Background

At the SAFE Commission meeting in August, I presented a very simple overview of cyber threats and discussed the design principles for secure voting systems. A copy of that PowerPoint is on the SAFE Commission website with a transcript from the August meeting.

Below, I offer a reference document for all Commissioners, which is: I.) a summary of basic security requirements for a secure voting system, II.) a comparison of the two main approaches under discussion (namely, hand-marked paper ballots vs. a ballot-marking device with paper printouts), III.) a description of the current consensus among computer scientists for a voting system based on hand-marked paper ballots, and IV.) a proposal that the State of Georgia consider cost-effective measures, such as leasing – instead of purchasing – voting machinery.

I. Basic Security Requirements

Strong Software Independent

A voting system must ensure that each voter's vote is counted accurately. That is, the vote is cast in the voting system as intended by the voter, is collected by the voting system as cast, and is counted by the voting system as collected.

The most critical cybersecurity risk in a voting system is that votes are not counted accurately as a result of cyberattacks. Therefore, a voting system must be "strong software independent," that is:

- an undetected change or error (including cyberattack) in software cannot cause an **undetectable** change or error in an election outcome; and
- a detected change or error (due to poor software performance or cyberattack) can be corrected without re-running the election.

The only way to achieve "strong software independent" status is for the voting system to maintain a trail of voter evidence that cannot be tampered or deleted by **any** software component (including data within a device, data in transit, and data at rest on a server).

Continued…

Paper Ballots

A voting system must use paper ballots as the durable, independent evidence to verify or determine the correct election outcome, by ensuring that the paper ballots have accurately captured the voters' intended votes and that the custody of the paper ballots is secure.

With paper ballots, we can apply risk-limited-auditing to verify or determine the correct election outcome, that is, we can continue to examine random samples of ballots and manually count the votes, until:

- there is strong statistical evidence that the election outcome is correct, (i.e., the results of manual counting agree with the results of a tallying cyber system), or
- there has been a complete manual tally. In this case, the tallying cyber system must have functioned improperly either due to a cyberattack or some other error, and we turn to the complete manual tally as the correct election outcome.

In order to support risk-limited-auditing, paper ballots must be easily and clearly readable and manually countable. In particular, a paper ballot must show each and every vote exactly as the cast by the voter. It cannot be just a summary of the votes (e.g., only a tally, or only the presidential ballot and not the down ballots). A manual count absolutely cannot rely upon a barcode, QR code, or any other kind of encoding scheme that is readable only by a machine because the cyber system that reads those codes also can be compromised and lie to the voter or auditor. In short, during a manual review, a human must be able to clearly see evidence of the voter's original act.

II. Hand-Marked Paper Ballots vs. Printouts from a Ballot-Marking Device

In order to ensure that paper ballots accurately capture voter intent, **the best approach is to require the voters to hand mark paper ballots that are then scanned and tallied by cyber system but also dropped into a safe box.** This is because marking each vote captures and verifies the voter's intention in a single act.

The much less desirable approach is to have a voter cast his vote on a ballot-marking device, with a cyber component, and print out a paper receipt that the voter would verify and also drop into a safe box. This approach is not secure because the ballot-marking device may have a vulnerability that could be exploited to change votes. Asking the voter to read a printout receipt as verification of his/her action is an additional step that simply could be ignored by the voter.

The difference between these two approaches is critical: With hand-marked paper ballots, a voter both casts and verifies (that is, the voter verifies as s/he marks and cannot cast without already verifying). However, with ballot marking devices, the voter can easily skip the verification step.

III. Consensus Opinion Among Computer Scientists

A steady stream of election security studies by independent, non-profit and/or academic researchers has been produced in the past decade, and especially during the past two years.

These studies offer what is now a well-developed consensus from cybersecurity researchers and computer scientists across the United States who agree that a secure voting system should work as follows:

1. A voter is given a paper ballot.
2. S/he marks the intended vote.
3. S/he then puts the ballot on a scanner to have a machine record the vote.
4. Once scanning is done, the voter also drops the ballot into a safe box.
5. The scanning machine forwards the recorded votes to a tallying machine, which counts the votes from all voters and outputs the election result.
6. Auditors may then open the safe box to perform a risk-limiting audit, (i.e., manually read and count samples to verify that outputs from the tallying system are correct).

See "Additional Sources & Studies" at the end of this document for links to studies and handbooks for election officials.

At the 2018 Georgia Tech Cybersecurity Summit (held on October 4, 2018), Mr. Michael Morell, former acting director of the CIA, told the audience that our "failures to imagine" how our adversaries would attack us have been our biggest and most devastating failures as a nation (e.g., the 9/11 terrorist attack and the DNC server hack, to name two). Therefore, we must take the threat of cyberattacks against voting systems very seriously even though there is not yet proof that past cyberattacks have affected any election outcome in the United States.

Mr. Morell also revealed that, at the CIA, the top most secret information is now held on paper only; he said, "We are going back to paper." Therefore, given that we must protect the integrity of votes, requiring voters to hand-mark and verify votes on paper ballots is the most prudent approach.

IV. Additional Security and Fiscal Considerations: Leasing & Print-on-Demand

Given the importance of cybersecurity, a voting system must use the latest generation of hardware and operating-system technologies, many of which are designed to provide stronger security protection than the previous generations of such technology. Instead of purchasing a system and using it for nearly 20 years, the State of Georgia should consider leasing a voting system, for example, every five years or less. This helps to ensure that Georgia uses the most up-to-date technology available. It also applies pressure to vendors to keep their products up-to-date. The option of lease vs. purchasing also alleviates the need for the State of Georgia to appropriate such a dramatic volume of funds (estimated to be $30M - $100M+) at one time for the purchase of a voting system.

At the August 2018 public meeting of the SAFE Commission, we heard that other areas of the country have effectively used print-on-demand features to reduce the cost of paper ballots. A cited example was that of King County (metro Seattle) – an industrious area that includes metropolitan Seattle and the headquarters of technology leaders Amazon and Microsoft. Of note is that King County reduces paper waste and the financial cost of unnecessarily printed,

paper ballots by equipping polling stations with an electronic copy of an official, certified paper ballot. Such an approach in the State of Georgia would allow the Secretary of State's office to certify the official ballot for each County, provide a human-readable copy for reference by poll workers, and provide an electronic copy for print-on-demand as voters arrive. A print-on-demand approach alleviates the financial and logistical burden of providing thousands of paper ballots (which may go unused) to 159 counties.

Summary

We need a voting system that can recover from any cyberattack without the need to rerun the election. Such a system will give voters the confidence that their votes will never be compromised by cyberattacks. This can be achieved by making the voting system "strong software independent," which in turn requires paper ballots as the durable, independent trail of voter intent that can be manually audited by humans (through sampling and counting). Paper ballots must be easily and clearly readable and manually countable; a paper ballot must show each and every vote exactly as the voter cast it.

A secure voting system should use hand-marked paper ballots instead of ballot marking devices. That is, voters hand-mark their paper ballots, submit the paper ballots to the scanning machine, and once scanned drop them into a safe box. This approach guarantees that the voters verify their intended votes while casting the votes, and the risk-limiting auditing process will guarantee that the votes are collected and counted accurately. This consensus approach among the cybersecurity research community ensures that votes by the voters are counted accurately.

Instead of purchasing a voting system that is used for many years, the State of Georgia should lease a new system every few years to ensure its voting system is built on top of the latest generation of security technologies provided via the latest hardware and operating systems.

Acknowledgement

I have borrowed important concepts, in particular, "strong software independent," from the report "Public Evidence from Secret Ballots" (see https://arxiv.org/abs/1707.08619). One of its primary authors is Professor Ron Rivest at the Massachusetts Institute of Technology and the "R" of RSA, the most widely-used public-key cryptography algorithm. Professor Rivest is also a winner of the Turing Award, internationally recognized as the "Nobel Prize" for computer science.

For Reference

Questions to Ask Potential Vendors

At the August meeting, vendors expressed a willingness to customize a secure voting solution for the State of Georgia. In addition to the Request for Information by the Georgia Secretary of State's office (dated Aug. 20, 2018), worthwhile questions surrounding cybersecurity to ask a prospective voting or election system vendor are:

- What internal cybersecurity practices do you follow within your organization? How do those compare to the standards recommended by the National Institute of Standards and Technology at the U.S. Dept. of Commerce?
- What cyberattack(s) has your organization experienced in the past 24 mos., and how were they managed?
- What is your process for identifying new cybersecurity threats to your products? How are those cyber vulnerabilities managed and rectified? How are they reported to prior customers?
- What percent of your product was developed in-house by your organization? Which portions were developed by sub-vendors?
- How are sub-vendors involved in cybersecurity updates (i.e., code, patches, controls, etc.)?
- How will you collaborate with the State of Georgia to mitigate any security risks that we identify, as well as respond to a unique cyberattack in Georgia involving your product?
- When was your product launched? When was it last updated? When do expect to perform the next significant update to this technology?

Recommended Requirements of Vendors

per guidance by the Harvard Kennedy School Belfer Center for Science and International Affairs

IDENTIFY

- **Examine all the possible functionalities of the device** and of any of its subcomponents. Specifically pay attention to the wireless and networking functionality.
- **Know the certification status of all your equipment.** The Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG) provides federal level certification standards. Many states have their own certification process.

PROTECT

- **If you have a DRE machine that does not produce a paper trail, you should either replace the device or purchase an add-on (VVPAT adapter) that creates a paper trail.**
- **Physical Security/Access Seals**. Use serialized tamper-evident security seals and chain of custody logs to limit physical access to voting machines and track whenever removable media is plugged into the scanners.
- **Penetration test systems**. Conduct, or hire a third-party firm to conduct, a source code audit and penetration test of all vote-casting devices.
- **Restrict device functionality to what is required**. Even if you have disabled a feature through a settings page (such as Wi-Fi connectivity), those features could still be

exploited. You should not trust that toggling a switch in software actually will disable the functionality. If possible, the hardware should be removed.

- **Isolate the device from external connectivity. Do not connect the device to a network, which includes not using a cellular modem.** If network connectivity cannot be avoided, make sure to keep the network connection disabled until you intend to transmit the results.
    - **Create a copy of the results** (either a printout or by saving it to removable media) before you connect to the network.

- If removable media is used to transfer data (e.g., ballot definition files, vote tallies):
    - **Have a procurement strategy for devices**. Purchase physical media devices directly from a trusted vendor and obtain assurance that the suppliers from whom your vendors procure their memory can also be trusted. If you must use devices from an unverified source, obtain them from a location that you would not otherwise use, to make it less likely that a bad actor could plant USB devices that could infect your systems.
    - **Protect device chain of custody**. Once devices are procured, ensure that they are stored securely and access is limited to the appropriate audience. When in use, maintain a physical record of the device—including where the device has been and who has been in contact with it— to limit the opportunity for manipulation.
    - **One-way/one-time use**: Only use physical media once, from one system to a second system, then securely dispose of it. A USB device could either (1) transfer data from one air-gapped machine to another or (2) transfer data from an air-gapped machine to an outside one prior to disposal, but not both. When feasible, use write-once memory cards or write-once optical disks instead of USB devices. This ensures one-time use is self-enforced by the technology.
    - **Scan media devices** for malware. If you detect abnormalities, don't use the device and contact forensic experts for assistance.

DETECT

- Perform logic and accuracy testing of the programmed device.
- Verify the seals and chain of custody logs via a unique identifier (e.g., seal number).

RESPOND & RECOVER

- Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Continued…

VENDOR CONSIDERATIONS

- Vendors are integral to vote casting devices as every device has been physically constructed, programmed, and is often maintained by various vendors. A compromise or oversight at any of these points would allow an attacker to change or erase election results.
- See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in *Appendix 1: Vendor Selection and Maintenance*.

Additional Sources & Studies

- Center for Election Innovation & Research. September 2018. *Voter Registration Database Security.* Washington, DC: CEIR. https://electioninnovation.org/2018-vrdb-security/

- National Academies of Sciences, Engineering, and Medicine. September 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25120

- DEF CON Voting Village 26. September 2018. *Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure.* Las Vegas: DEF CON. https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf

- Harvard Kennedy School Belfer Center for Science & International Affairs. February 2018. *Defending Digital Democracy: The State & Local Election Security Playbook: Technical Recommendations.* Cambridge, Mass.: Harvard Press. https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

- Center for Internet Security. February 2018. *A Handbook for Elections Infrastructure Security.* East Greenbush, NY: CIS. https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

- *Public Evidence from Secret Ballots*. In Proceedings of the Second International Joint Conference for Electronic Voting (E-Vote-ID), October, 2017. Lecture Notes in Computer Science 10615, Springer. Also available at https://arxiv.org/abs/1707.08619

###