Email and Internet Voting: The Overlooked Threat to Election Security

This report reviews the research that has been conducted by the federal government concluding that secure online voting is not yet feasible.

SHARE

Download Email and Internet Voting: The Overlooked Threat to Election Security

Executive Summary

Over the past two years, revelations that our election systems have been targeted for cyberattack have roiled the U.S. Leaders of our national security apparatus have repeatedly warned that our election infrastructure continues to be targeted for online attacks by foreign intelligence. As state election officials grapple with the looming threat of cyberattack on election technology, there is a significant vulnerability that has been roundly ignored: transmission of ballots over the internet, including by email, fax and blockchain systems.

This report reviews the research that has been conducted by the federal government concluding that secure
online voting is not yet feasible. We examine the insoluble security problems that are inherent to casting ballots online, including server penetration attacks, client-device malware, attacks to emailed and faxed ballots in transit, denial-of-service attacks, disruption attacks and the challenge to reliably authenticate voters.

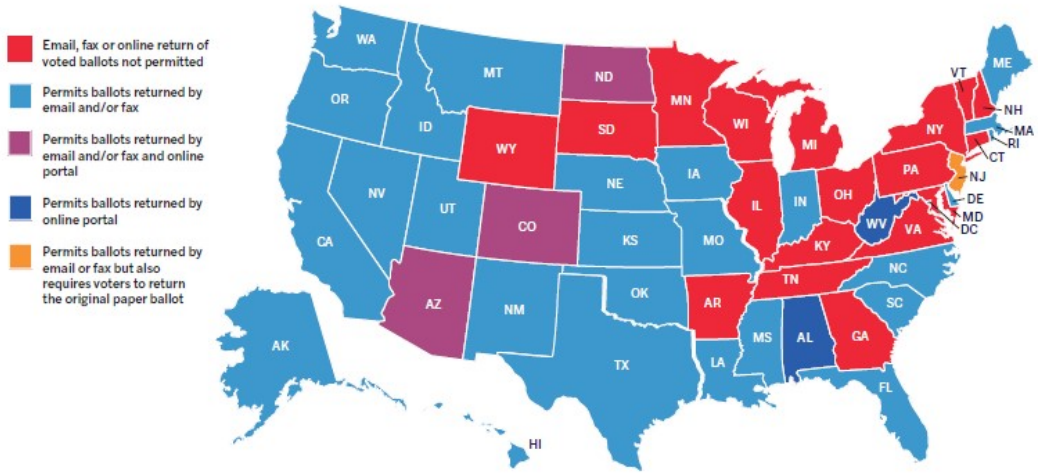
The report foregrounds a serious, yet widely overlooked cybersecurity threat to state and county election infrastructure that receive ballots sent as attachments in the form of emails or digital faxes. In jurisdictions that receive ballots by PDF or JPEG attachment, election workers must routinely click on documents from unknown sources to process emailed or faxed ballots, exposing the computer receiving the ballots — and any other devices on the same network — to a host of cyberattacks that could be launched from a false ballot laden with malicious software. An infected false ballot would enter the server like any other ballot, but once opened, it would download malware that could give attackers backdoor access to the elections office's network.

A review of publications on security best practices from the U.S. Election Assistance Commission (EAC), the Department of Homeland Security (DHS) and the National Association of Election Officials found no published guidance regarding the security of emailed ballots or recommendations for securing a computer terminal receiving emailed ballots.

Findings:

- Federal government, military and private sector studies have examined the feasibility of internet-based voting and have concluded it is not secure and should not be used in U.S. government elections.
- Thirty-two states permit online voting for some subset of voters.
- In the 2016 general election, over 100,000 ballots were reported to have been cast online, according to data collected in the EAC's Election Administration and Voting Survey. The actual number is likely much higher.
- The federal agencies supporting states in improving their election security have not issued any warnings regarding the online return of voted ballots.
- Ballots returned online can be undetectably changed by a variety of cyberattacks, including via malware on a user's computer and server penetration attacks. The latter has been demonstrated live and in a "test" election.
- Internet voting expands the opportunity for an attacker to engage in damaging disruption and denial-of-service attacks, aimed at disabling the system, prohibiting voters from casting ballots, and undermining voter trust in the election.
- Receiving ballots as attachments can also expose a state or county election system to systemic election system attacks. Sophisticated attackers can spoof a legitimate voter's emails and use fake ballots to deliver malware that can be used to gain entry into county or state election infrastructur
- New technologies, including blockchain, fail to resolve the insoluble security issues inherent with online voting. These issues include server penetration attacks, client-device malware, denial-of-service attacks and disruption attacks.

SHARE



Copyright 2018 Common Cause. All Rights Reserved. Privacy Policy

Conclusion

Until there is a major technological breakthrough in or fundamental change to the nature of the internet, the best method for securing elections is a tried-and-true one: mailed paper ballots. Paper ballots are not tamper-proof, but they are not vulnerable to the same wholesale fraud or manipulation associated with internet voting. Tampering with mailed paper ballots is a one-at-a-time attack. Infecting voters' computers with malware or infecting the computers in the elections office that handle and count ballots are both effective methods for large-scale corruption.

Military voters undoubtedly face greater obstacles in casting their ballots. They deserve any help the government can give them to participate in democracy equally with all other citizens. However, in this threat-filled environment, online voting endangers the very democracy the U.S. military is charged with protecting.

Considering current technology and current threats, postal return of a voted ballot is the most responsible option. States that permit online return of voted ballots should suspend the practice. Federal agencies such as DHS and EAC should acknowledge the vulnerabilities introduced by permitting online voting and recommend that states curtail all online ballot return. Until they do, the integrity of Americans' votes are at stake, and in many cases, the integrity of the election system is at risk.

SHARE

Summary Recommendations

We recommend some basic precautions that election officials and voters should follow. [A comprehensiv set of recommendations is at the end of this report.]

Recommendations for election administrators:

- Map the network to ensure that the computer used to receive emailed or digitally faxed ballots is *not* connect- ed to or on the same network as the voting machine network, election management system (EMS) or voter registration system through the wired or wireless means.
- Scan all incoming email and digital attachments formalware. The mail program should be configured to verify that attachments are of the expected type and fall into the typical size range. Important: Scanning may find attachments for executable malware programs but may be unable to detect malware *inside* a PDF or JPEG file. Malware inside such files is much more complex.
- Ensure all ballots returned by electronic means are printed for counting and not electronically transmitted to the EMS for tallying.
- Provide all voters with information and options for mailing ballots back by postal mail.
- Ensure military voters are aware of the free expedited postal mail option available to them. Recommendations for voters:
- Voters who receive blank ballots in the mail are encouraged to mark the ballots and mail them back.
- Voters who receive blank ballots by email are encouraged to print out the ballot and mark it by hand if possible. If marking the ballot using a computer, print out the final version and carefully review the choices before mailing it back.
- Send the ballot back by postal mail. Military personnel in army, fleet or diplomatic post office (APO/FPO/ DPO) locations can return absentee ballots via Priority Mail Express using the free

Express Mail Label 11-DOD.

After the 2018 general election, states that permit online return of voted ballots should eliminate the practice. This will require legislative action in most states. While imposing a quarantine on incoming ballots is helpful, that will by no means stop a sophisticated attacker from attempting to use ballots in a spear phishing attack or corrupting ballots in transit. Additionally, federal agencies charged with assisting states in strengthening their election security should exercise leadership and publish warnings regarding the online return of voted ballots.

Download Email and Internet Voting: The Overlooked Threat to Election Security

Site by Wide Eye Creative

SHARE