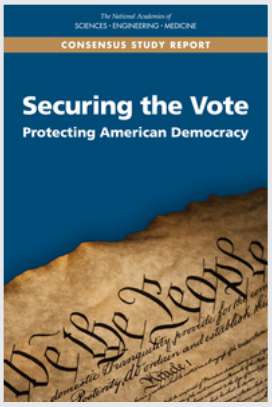

Securing the Vote: Protecting American Democracy (2018)

DETAILS

180 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-47647-8 | DOI 10.17226/25120

CONTRIBUTORS

Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology; Committee on Science, Technology, and Law; Policy and Global Affairs; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

5

Ensuring the Integrity of Elections

In this chapter, the committee discusses threats to the integrity of U.S. elections. Two topics that play critical roles in protecting this integrity, cybersecurity and auditing, are considered. The committee then assesses the widely proposed suggestion that ballots be cast via the Internet.

INTRODUCTION

There are numerous ways in which the integrity of elections can be affected. Election results may be improperly tallied or reported. Inaccuracies may be introduced by human error or because of a lack of proper oversight. Vote counts can be affected if fraudulent voting, e.g., multiple voting, illegal voting, etc., occurs. Election tallies and reporting may also be affected by malicious actors.

Malicious actors can affect vote counts by:

- introducing inaccuracies in the recording, maintenance, and tallying of votes; and/or
- altering or destroying evidence necessary to audit and verify the correct reporting of election results.[1]

There are many ways to prevent the casting of votes. Voters can be physically barred or otherwise deterred (e.g., by intimidation) from access-

[1] Other threats, e.g., disinformation campaigns, gerrymandering, etc., may affect election integrity and, while important, were viewed by the committee as outside of its charge.

ing polling sites. Information on voting locations, voting times, and voting processes may be manipulated to mislead potential voters. Disruptions in mail or Internet service may adversely affect remote voters. Registration data may be altered to disenfranchise voters. Voting equipment failures or inadequate supplies could prevent vote collection.

After votes have been cast, physical or electronic ballots can be altered, destroyed, or lost. Counting errors may affect manual or electronic tallying methods. Tallies may be inaccurately reported because of carelessness or malicious activity.

After the primary reporting of results, evidence that enables verification of the reported results may be altered or destroyed. This evidence could include original artifacts (e.g., cast ballots) or supplemental data provided to enable external auditing and verification.

Disruptions of Electronic Systems

Security vulnerabilities can be exploited to electronically disrupt voting or affect vote counts at polling locations or in instances of remote voting.

Denial-of-service Attacks

Denial-of-service (DoS) attacks interrupt or slow access to computer systems.[2] DoS can be used to disrupt vote casting, vote tallying, or election audits by preventing access to e-pollbooks, electronic voting systems, or electronic auditing systems.

When employed against even a limited number of jurisdictions, DoS disruptions could lead to a loss in confidence in overall election integrity. A DoS attack targeting select jurisdictions could alter the outcome of an election.

Malware

Malware—malicious software that includes worms, spyware, viruses, Trojan horses, and ransomware—is perhaps the greatest threat to electronic voting.[3] Malware can be introduced at any point in the electronic path of a

[2] If equipment is manipulated to slow its operation or compromise its operability, this may also constitute a DoS attack.

[3] Worms are standalone computer programs that replicate themselves in order to spread to other computers, possibly compromising the operability of the computers they infect now or in the future. Spyware is software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge. A computer virus is a type of malicious software program that, when executed, replicates

vote—from the software behind the vote-casting interface to the software tabulating votes—to prevent a voter's vote from being recorded as intended.

Malware can prevent voting by compromising or disrupting e-pollbooks or by disabling vote-casting systems. It can prevent correct tallying by altering or destroying electronic records or by causing software to miscount electronic ballots or physical ballots (e.g., in instances where optical scanners are used in the vote tabulation process). Malware can also be used to disrupt auditing software.

Malware is not easily detected. It can be introduced into systems via software updates, removable media with ballot definition files, and through the exploitation of software errors in networked systems. It may also be introduced by direct physical access, e.g., by individuals operating inappropriately at points during the manufacturing of the election system or at the level of elections offices. It is difficult to comprehensively thwart the introduction of malware in all these instances.

Other Classes of Attacks

There are other avenues through which electronic systems may be disrupted. Malicious actors may obtain sensitive information such as usernames or passwords by pretending to be a trustworthy entity in an electronic communication. Servers may be breached to obtain administrator-level credentials. Individuals with site access (e.g., employees or contractors) might physically access a system.

Maintaining Voter Anonymity

If anonymity is compromised, voters may not express their true preferences. Anonymity can be compromised in many ways. Clandestine cameras at poll sites could be used to compromise voter anonymity. Latent fingerprints left on ballots might be used to link voters to their ballots. Full ballots dissociated from individual voters might be posted in the interest of ensuring transparency and/or to facilitate auditing, but it may be possible to tie particular ballots to individual voters. When voter anonymity is achieved using encryption, a failure in the encryption can lead to the disclosure of a voter's identity. With remote voting—voting outside of publicly monitored poll sites—it may not be difficult to compromise voter privacy. When voting, for example, by mail, fax, or via the Internet, individuals can

itself by modifying other computer programs and inserting its own code. Trojan horses are malicious computer programs that mislead users of their true intent. Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

be coerced or paid to vote for particular candidates outside the oversight of election administrators.

ELECTION CYBERSECURITY

Overview and Analysis

As described in Chapter 1, the Help America Vote Act (HAVA) prompted the acceleration of the introduction of electronic systems throughout the U.S. election process. There have since been concerns about vulnerabilities in the electronic systems that are used to perform most election functions. Given competing demands for attention and resources, these concerns have not always been a high priority for election administrators. However, citizen and government attention to these vulnerabilities greatly increased following reports of Russian efforts to compromise voter registration systems during the 2016 presidential election.

Attention brought to the problem of election cybersecurity during the 2016 election prompted energetic reactions from government, academia, and the public and private sectors. Following the U.S. Department of Homeland Security (DHS) designation of elections as critical national infrastructure, election administrators established the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to improve information sharing among election officials. In addition, governmental and private-sector coordinating councils were established to share information and engage with DHS to address cyber threats to elections. In addition, organizations such as the Center for Internet Security and the Belfer Center at Harvard University have issued guides and "playbooks" to assist state and local officials in the mitigation of risks to their electronic system and in the adoption of best security practices.[4] Most recently, as part of the omnibus FY 2018 appropriations bill, the U.S. Congress appropriated $380 million "to the Election Assistance Commission for necessary expenses to make payments to States for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements."[5]

Election administrators face a daunting task in responding to cyber threats, as cybersecurity is a concern with all computer systems. This is

[4] See The Center for Internet Security, "A Handbook for Elections Infrastructure Security," available at: https://www.cisecurity.org/elections-resources/, and Belfer Center for Science and International Affairs, Harvard Kennedy School, "The State and Local Election Cybersecurity Playbook," available at: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

[5] See H.R. 1625, Consolidated Appropriations Act, 2018, Section 501, available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

because (1) the design and development of current computer systems, no matter how well constructed, cannot anticipate and prevent all the possible means of attack; and (2) there are parties that will act in deliberately hostile ways to exploit vulnerabilities.

Vulnerabilities arise because of the complexity of modern information technology (IT) systems and human fallibility in making judgments about what actions are safe or unsafe from a cybersecurity perspective. Moreover, cybersecurity is a never-ending challenge. It is unlikely that permanent protections against cyber threats will be developed in the near future given that cybersecurity threats evolve and that adversaries continually adopt new techniques to compromise systems or overcome defenses. The general view is that the offense has the upper hand if the attacker is patient and well resourced. With respect to foreign threats, the challenge is compounded by the great asymmetry between the capabilities and resources available to local jurisdictions in the United States and those of foreign intelligence services.

Unfortunately, not all vendors or jurisdictions follow established best practices with respect to the development, maintenance, and operation of voting systems. This makes them more vulnerable to cyber-manipulation than they need to be. In comparison with other sectors (e.g., banking), many jurisdictions in the election sector are not following best security practices with regard to cybersecurity, one reason being that the banking industry is highly regulated, and part of these regulations is the supervision of their cybersecurity strategies.[6]

Several factors affect a bad actor's ability to compromise a system: (1) how well the system was designed; (2) whether the system is properly configured and updated; (3) how well the system is managed and operated; and (4) the skills, resources, and determination of the would-be attacker. Adoption of best practices for developing, testing, and management of systems can reduce (but not eliminate) the risk of a successful cyberattack. As a rule, stronger defenses increase the time and effort required to conduct an attack, and well-defended targets are less attractive to would-be attackers.

There are many layers between the application software that implements an electoral function and the transistors inside the computers that ultimately carry out computations. These layers include the election application itself (e.g., for voter registration or vote tabulation); the user interface; the application runtime system; the operating system (e.g., Linux or Windows); the system bootloader (e.g., BIOS or UEFI); the microprocessor firmware (e.g., Intel Management Engine); disk drive firmware; system-on-

[6] See, e.g., https://www.occ.treas.gov/news-issuances/news-releases/2017/nr-occ-2017-113.html and https://www.csbs.org/sites/default/files/2017-11/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf.

chip firmware; and the microprocessor's microcode. For this reason, it is difficult to know for certain whether a system has been compromised by malware. One might inspect the application-layer software and confirm that it is present on the system's hard drive, but any one of the layers listed above, if hacked, may substitute a fraudulent application layer (e.g., vote-counting software) at the time that the application is supposed to run. As a result, there is no technical mechanism that can ensure that every layer in the system is unaltered and thus no technical mechanism that can ensure that a computer application will produce accurate results. This has several important implications for election systems:

- all digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists—is subject to malicious alteration;
- there is no technical mechanism currently available that can ensure that a computer application—such as one used to record or count votes—will produce accurate results;
- testing alone cannot ensure that systems have not been compromised; and
- any computer system used for elections—such as a voting machine or e-pollbook—can be rendered inoperable.

Election systems are especially vulnerable when they are connected to the Internet, telephone network,[7] or another wide-area network.[8] Systems that utilize network connections for their functions include voter registration systems, e-pollbooks, and post-election canvassing/reporting systems.

Even when systems are not directly connected to networks, they are vulnerable to attack through physical or wireless access.[9] They also are vulnerable whenever data transferred to them originates from another computer system that is itself vulnerable. For example, to attack a voting machine that receives data only through hand-carried removable media bearing "ballot definition files," an attacker might create a ballot definition file that takes advantage of a flaw in the software that reads a ballot definition file or displays a ballot.[10] Such an attacker need not be physically

[7] The telephone network is actually now part of the Internet. Land-line switching centers and cell-phone towers connect to each other through packet-switched networks (i.e., the technology underlying the Internet) that are connected to the larger Internet via border routers.

[8] Most wide-area networks are also connected to the larger Internet.

[9] Attacks are possible not only when systems are in use for elections but also during the manufacturing process or when such systems are in transit or in storage.

[10] Essentially every type of electronic voting machine must be programmed with ballot designs shortly before an election. As such, this is a particularly tempting attack vector, particularly for sophisticated actors.

present with that removable media—entry through a network-connected computer that creates the removable storage media may suffice (the removable storage media is used to transmit the ballot definition file).

Achieving stronger defenses against cyberattacks involves: (1) adopting state-of-the-art technologies and best practices more widely; and (2) developing new knowledge about cybersecurity. The first defense is primarily nontechnical and involves economic, organizational, and behavioral factors. The second defense requires research to develop new technologies and approaches.[11]

Cybersecurity and Vote Tabulation

Because there is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats, one must adopt methods that can assure the accuracy of the election outcome without relying on the hardware and software used to conduct the election. Uniform adoption of auditing best practices does not prevent tampering with the results collected and tabulated by computers. It can allow such tampering to be detected and often corrected. Good auditing practices can demonstrate that the results of an election accurately reflect the intention of the electorate without a need to trust the equipment used to conduct the election.

Cybersecurity and E-pollbooks

With respect to e-pollbooks and other election systems used during the election, independent backup systems are necessary in the event that primary systems become unavailable. E-pollbook data have traditionally been backed up with paper printouts. As an alternative, databases might be stored on static media such as DVDs. However, in jurisdictions that offer same-day registration or convenience voting in self-selected locations, relying on paper could lead to new risks of in-person voter fraud.[12] Addressing this risk by building fully independent systems (including independent networks connecting the polling sites) is not practical.[13]

[11] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (National Academies Press, Washington DC: 2014).

[12] While paper pollbooks will not proactively stop some forms of multiple voting, their use permits the retroactive detection of such activity and provides evidence against those acting illegally.

[13] In practice, there is no such thing as an independent network. See, e.g., footnote 7.

Factors that Exacerbate Cybersecurity Concerns

- *A highly decentralized elections system*. Because the U.S. elections system is highly decentralized, responsibility for cybersecurity often falls to the county or municipal level where expertise and resources may be quite limited.
- *Aging systems*. Because U.S. elections frequently make use of hardware and software that are aging—in some cases to the point that they would generally be considered obsolete—cybersecurity risk is increased because (1) such systems may fall well behind the current state of the art in cybersecurity measures; and (2) software or the operating system used to run it may no longer be receiving security updates.
- *Changing threat*. Traditionally, the goal has been to secure against election fraud by corrupt candidates or their supporters who may attempt to favor a particular candidate by altering or destroying votes or tampering with the vote tally. The 2016 election vividly illustrated that hostile state actors can also pose a threat. These actors often possess more sophisticated capabilities and can apply greater resources to the conduct of such operations. Moreover, they may have other goals than shifting the outcome for a particular candidate. If their goal is to disrupt an election or undermine confidence in its outcome, they may need only to achieve DoS against e-pollbooks or leave behind traces of interference like malicious software or evidence of tampering with voter registration lists or other records. Even failed attempts at interference could, if detected, cast doubt on the validity of election results absent robust mechanisms to detect and recover from such attacks.

Findings

There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats.

U.S. elections are conducted using systems that are aging and prone to security vulnerabilities and operational failures. The continued use of outdated systems increases the possibility of a critical failure. Even if actual failures or compromises do not occur, there is a risk that public confidence in the electoral process could be undermined by the possibility of such compromise—especially if there are indications that such a compromise was attempted.

In comparison with other sectors (e.g., banking), the election sector is not following best security practices with regard to cybersecurity.

Data discrepancies are more difficult to detect in elections than in most other sectors because voters do not generally learn whether their votes were processed correctly.[14]

Even if best practices are applied, systems will not be completely secure.

Foreign state–sponsored attacks present a challenge for even the most responsible and well-resourced jurisdictions. Small, under-resourced jurisdictions are at serious risk.

Appropriate audits can be used to enable trust in the accuracy of election outcomes even if the integrity of software, hardware, personnel, or other aspects of the system on which an election is run were to be questioned.

Better cybersecurity is not a substitute for effective auditing.

RECOMMENDATIONS

5.1 Election systems should continue to be considered as U.S. Department of Homeland Security–designated critical infrastructure.

5.2 The U.S. Election Assistance Commission and U.S. Department of Homeland Security should continue to develop and maintain a detailed set of cybersecurity best practices for state and local election officials. Election system vendors and state and local election officials should incorporate these best practices into their operations.

5.3 The U.S. Election Assistance Commission should closely monitor the expenditure of funds made available to the states for election security through the 2018 omnibus appropriations bill to ensure that the funds enhance security practices and do not simply replace local dollars with federal support for ongoing activities.[15] The U.S. Election Assistance Commission should closely monitor any future federal funding designated to enhance election security.

5.4 Congress should provide funding for state and local governments to improve their cybersecurity capabilities on an ongoing basis.

ELECTION AUDITING

Overview and Analysis

Election audits are critical to ensuring the integrity of election outcomes and for raising voter confidence. Auditing can demonstrate the validity of

[14] End-to-end-verifiable systems have the capacity to demonstrate to voters that their votes were properly counted.

[15] See H.R. 1625, Consolidated Appropriations Act, 2018, Section 501, available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

an election outcome and provide an indication of errors in ballot tabulation. Effective auditing contributes to voting security by providing an answer to the question, "Can we trust the outcome of an election when the equipment (hardware and software) used to conduct the election may have vulnerabilities or when the process is subject to human error?"

For decades, traditional audits have been performed (and have been required by law) in many states. While election administrators have performed many types of post-election audits, such as process audits, the most widely known audits have been audits of cast ballots. Traditional ballot auditing requires that election results in some fixed percentage of precincts be reconfirmed by a hand count—though the details of actual implementation can reduce the value of the audit (election administrators should not, for example, always audit the same precincts).

Hand counting every ballot cast to be certain of the outcome is extremely time-consuming, and hand counts are susceptible to error or deliberate miscounting. The use of computerized voting machines provides flexibility and processing efficiencies. Nevertheless, computers are, as was discussed in the previous section, subject to programming errors, manipulation, and outside interference. Election audits have, therefore, become more important, as the performance of audits raises voter confidence in the reported outcomes of elections. The use of networked communication at various election stages has necessitated audits that address cybersecurity risks.

An evidence-based election would produce not only a reported (or initial) election outcome, but also evidence that the reported outcome is correct. This evidence may be examined in a "recount" or in a "post-election audit" to provide assurance that the reported outcome indeed is the result of a correct tabulation of cast ballots.

Voter-verifiable paper ballots provide a simple form of such evidence provided that many voters have verified their ballots. The ability of each voter to verify that a paper ballot correctly records his or her choices, before the ballot is cast, means that the collection of cast paper ballots forms a body of evidence that is not subject to manipulation by faulty hardware or software. These cast paper ballots may be recounted after the election or may be selectively examined by hand in a post-election audit. Such an evidence trail is generally preferred over electronic evidence like electronic cast-vote records or ballot images. Electronic evidence can be altered by compromised or faulty hardware or software.

Paper ballots are designed to provide a human-readable recording of a voter's choices. The term "paper ballot" here refers to a "voter-verifiable paper ballot," in the sense that voters have the opportunity to verify that their choices are correctly recorded before they cast their paper ballots. The voter may mark the ballot by hand, or the marked ballot may be produced by a voting machine. In the current context, the human-readable

portion of the paper ballot is the official ballot of record that acts as the record of the voter's expressed choices.[16] Any human-readable, durable, tamper-evident medium such as cloth, cardstock, or plastic could be used instead of paper.

Statistical auditing techniques available now (and some in development) are more efficient and effective than earlier techniques wherein a predetermined percentage of precincts were recounted by hand to confirm the accuracy of initial precinct tallies. The implementation of statistical auditing techniques may require the allocation of additional time between the end of voting and when the official results of the election are certified.

Risk-Limiting Auditing

Auditing a fixed percentage of precincts may not provide adequate assurance with regard to the outcome of a close election. To address this weakness, a method of auditing known as risk-limiting auditing was developed.[17] Risk-limiting audits (RLAs) operate dynamically by examining individual randomly selected paper ballots until sufficient statistical assurance is obtained. This statistical assurance ensures that the chance that an incorrect reported outcome escapes detection and correction is less than a predetermined risk limit.

RLAs offer statistical efficiency. Auditing an election with tens of millions of ballots may require examining by hand as few as several hundred randomly selected paper ballots. A RLA might determine that more ballots need to be examined, or even that a full hand recount should be performed, if the contest is close or the reported outcome incorrect. Because RLAs layer a security mechanism (the risk-limiting audit itself) on top of the traditional vote-casting process, RLAs can often be performed without the adoption of new vote-casting processes. RLAs were piloted statewide in Colorado in 2017 and are now being piloted by several other states.[18]

---

[16] Rather than, for example, an electronic interpretation of the paper ballot or a non-human-readable barcode appearing on a ballot.

[17] For a general discussion of risk-limiting audits, see Lindeman, Mark and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security and Privacy*, Special Issue on Electronic Voting, 2012.

[18] The changes required to implement risk-limiting audits incur costs and require detailed planning, education, and development of required resources. Some states will, for example, need to adopt paper balloting (or purchase different scanners to be able to use comparison-based audits).

Executing an RLA for a single plurality contest in a single jurisdiction is not particularly challenging. Implementing an RLA for an election with multiple contests, multiple jurisdictions, multiple types of equipment, and multiple election types (not just plurality), requires more preparation, and a state (or other jurisdiction) should expect that the implementation process will take time.

The most efficient RLAs (comparison audits) make use of cast-vote records (CVRs) that electronically represent the contents of each paper ballot. A ballot-comparison audit operates by randomly selecting paper ballots from a list of all cast paper ballots on a ballot manifest and comparing the voter-verified human-readable contents of the selected paper ballots to the electronic records in the corresponding CVRs. When CVRs are not available (or cannot be linked to specific corresponding paper ballots), a ballot-polling audit may be used instead when margins are relatively large. Such an audit examines only randomly selected paper ballots (and no CVRs); however, many more paper ballots may need to be sampled and examined to achieve the same statistical assurance.[19]

RLAs can establish high confidence in the accuracy of election results—even if the equipment that produced the original tallies is faulty. This confidence depends on two conditions: (1) that election administrators follow appropriate procedures to maintain the chain-of-custody and secure physical ballots—from the time ballots are received, either in-person or by mail, until auditing is complete; and (2) that the personnel conducting the audit are following appropriate auditing procedures and the equipment and software used to audit the election are independent of the equipment and software used to produce the initial tallies. In the latter case, this not only requires that the software be independent of the software used to tally votes, but also that the software's specifications/algorithms, inputs, and outputs are transparent to permit members of the public to reproduce the software's operation.

End-to-end-verifiability

In recent years there has been increased interest in providing voters with an opportunity to verify that their votes have been accurately cast, counted, and tabulated. This presents a challenge due to the necessity of preserving the secrecy of the ballot. However, building upon cryptographic methods initially developed by computer scientist and cryptographer David Lee Chaum, researchers have developed an approach called end-to-end (E2E) verifiability. This approach enables voters and other members of the

In Colorado, the cost to the state to conduct its pilot of RLAs was $90,000 (Hall, Hilary, Boulder County (CO) Clerk and Recorder, presentation to committee, December 7, 2017, Denver, CO). Free & Fair, which developed the open-source tools used to conduct the Colorado RLA invested an additional $100,000 in the effort (Kiniry, Joe, Free & Fair, presentation to committee, December 7, 2017, Denver, CO).

[19] Not all optical scanners can produce CVRs that can be linked to specific paper ballots; linked CVR–based RLAs are more efficent and cost-effective than ballot-polling RLAs; therefore, the ability to produce linked CVRs is an important consideration when purchasing and deploying voting machines.

public to audit the integrity of an election without relying on hardware, software, or personnel associated with elections.[20]

An election is E2E-verifiable (E2E-V) if it achieves three goals: 1) voters can obtain assurance that their selections have been properly recorded; 2) any individual can verify that his or her ballots have been included in vote tallies; and 3) members of the public can verify that the final tally is the correct result for the set of ballots collected. E2E-verifiability enables not only detection of external threats, but also detection of internal threats including errors or tampering by election officials, corrupted equipment, or compromises originating with equipment vendors.

E2E-V voting systems adopt certain properties (see Box 5-1), encrypt ballot data, and permit verification of data throughout the voting process. In an election context, "end-to-end" refers to the flow of ballot data through the entirety of the voting process and to the idea that the data may be verified at multiple stages in the voting process. The phrase should not, however, be interpreted to mean that verification must occur at particular stages of the process.

E2E-verifiability is a property that may be achieved in an election—rather than a particular methodology. Systems with various characteristics have been designed to produce E2E-V elections. In practice, an E2E-V voting system might work as follows:

> Upon marking a ballot, the voter would obtain a receipt which is a "cryptographically-masked" copy of the voter's selections (the voter's choices would thus not be visible in a way that would enable vote-selling or coercion). The receipt could be machine-issued or derived from the process of marking a pre-printed paper ballot.
>
> There are several methods to test whether the encryption process is working properly. In one scenario, voters might be allowed to "spoil" one or more ballots after receipts have been produced.[21] Voters could subsequently verify that receipts issued for spoiled ballots accurately reflect selections made. Because voting systems cannot predict whether a voter

[20] For a general discussion of end-to-end (E2E) election verifiability, see Benaloh, Josh, et. al, "End-to-end Verifiability," 2014, available at: https://pdfs.semanticscholar.org/4650/db843e0e90ca7ff54c7fe8e6080d12f6a0fc.pdf. Dr. Benaloh is a member of the committee that authored the current report. Dr. Ronald L. Rivest, who is also a member of the committee that authored the current report, was a co-author of the paper and has authored other papers on end-to-end verifiability.

[21] A *spoiled ballot* is a ballot that is invalidated and not included in the vote tally. Ballots might be spoiled accidentally or deliberately. A ballot may be spoiled in many ways (e.g., if the ballot is defaced, if invalidating stray marks are added to the ballot, etc.).

Voters would be permitted to verify the accuracy of the encryption only on spoiled ballots. This is to ensure that the verification process could not be used to reveal how individuals actually voted.

BOX 5-1
Properties of End-to-end-verifiable Voting Systems

End-to-end-verifiable (E2E-V) voting systems share the following security properties:

Integrity. Once a voter successfully enters his or her ballot into an E2E-V system, it cannot be undetectably lost or modified in any way, even in the presence of computer bugs or malicious logic.

Counting Accuracy. Ballots cannot be miscounted without the miscount being detectable.

Public Verifiability. E2E-V systems provide outputs and publish sufficient verification data to permit any voter to verify that his or her ballot was not lost or modified and that votes were properly tabulated. Verification data provides cryptographic proof that ballot integrity was preserved and tabulation was correct. Anyone may run a verification program on the verification data to confirm the accuracy of the data.

Transparency. Mathematical principles underlying the E2E-V security guarantees are open and public. The specifications for verification programs are publicly documented, and voters and observers are free to create and execute their own verification programs.

SOURCE: Adapted from U.S. Vote Foundation, "The Future of Voting: End-to-end Verifiable Internet Voting," July 2015, p. 111, available at: https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf.
Dr. Ronald L. Rivest and Dr. Josh Benaloh, members of the committee that authored the current report, made contributions to the U.S. Vote Foundation report.

will spoil a ballot, a voting system must correctly encrypt all receipts, as only a small fraction of voters would need to verify that spoiled ballots have been properly encrypted to reveal systematic erroneous behavior by a voting system.

After polls close, copies of all voter receipts would be posted to a public electronic bulletin board in order to allow voters to confirm that their votes have been properly recorded. If the voter's unique receipt was not posted, the voter could file a protest and use the receipt as evidence for correcting the posting error.

All voter receipts would be processed using a series of cryptographic computations that would yield the results of the particular election. The algorithms and parameters for the cryptographic operations would be

posted on a website to enable voters to verify that their votes were tallied as recorded and to allow other observers to verify that the tally is correct.[22]

When E2E-verifiability is used with paper ballots, conventional recounts and risk-limiting audits are possible as additional means of verification.

E2E-verifiablility adds complexity to the election process, and the effective wide-scale deployment of E2E-verifiability will require a broad understanding of the underlying cryptographic methods by election officials and the general public. It may initially be challenging to understand the tools that could be employed to make E2E-verifiability possible.[23] Further, with E2E-V systems, it is possible that the encryption of voter receipts could be compromised. While such decryption would not affect the integrity of an election, it could compromise voter anonymity.

E2E-V methods seem to be necessary for secure voting via the Internet, but the methods are, in and of themselves, insufficient to address all of the security issues associated with Internet voting. Electronic versions of ballots may be subject to Internet-based (or other) attacks that might, for example, delete electronic ballots or otherwise replace or modify electronic election records. With E2E-V systems—as with any voting system—a bad actor could simply claim that his or her vote was not accurately captured. Such claims could eventually be discounted by security experts following the E2E-V trail of evidence. However, with sufficient numbers of bad actors acting simultaneously, confidence in an election outcome could be eroded before all the necessary independent verifications could take place.[24]

[22] Ali, Syed Taha and Murray, Judy, "An Overview of End to End Verifiable Voting Systems," in *Real-World Electronic Voting: Design, Analysis and Deployment*, Hao, Feng and Peter Y.A. Ryan, eds. (Boca Raton: CRC Press, 2016).

[23] For one fielded E2E-verification system (Scantegrity) used twice in elections in Takoma Park, MD, the voting process was seen as so much like that experienced previously with optical scan systems that voters did not notice the additional E2E-verifiability mechanisms. With other systems, it is possible that the impact of adding E2E-verification features would be more noticeable.

Scantegrity is paper-based insofar as the casting of ballots. It only uses the Internet as a means through which voters may verify that their votes were included in the tally, or by which anyone can verify that a vote tally is correct, given the posted votes.

[24] Some E2E-verifiable (E2E-V) systems provide mechanisms to address this threat. With the Scantegrity system, for example, voters mark their paper ballots with special pens that reveal a secret code when a voter selects a candidate (the code changes with each ballot). A voter cannot credibly claim to have voted for a candidate without knowing the associated code.

Findings

Complicated and technology-dependent voting systems increase the risk of (and opportunity for) malicious manipulation. Additional methods of review help reduce risks and detect violations of desired security properties.

Conducting rigorous audits enhances confidence in the correctness of election outcomes.

Risk-limiting audits can efficiently establish high confidence in the correctness of election outcomes—even if the equipment used to cast, collect, and tabulate ballots to produce the initial reported outcome is faulty.

States and jurisdictions purchasing election systems should consider in their purchases whether the system has the capacity to match CVRs to physical ballots, as this feature could result in future cost savings when audits are conducted.

While achieving E2E-verfiability, one must still preserve the secret ballot. E2E-V systems generally achieve this by using cryptographic methods to "mask" ballot data while preserving the ability for voters and observers to verify that ballots have been tallied correctly.

E2E-verifiability protocols are not, in and of themselves, sufficient to secure Internet voting, even in theory.

E2E-V election systems enable members of the public to conduct their own audits (or have audits conducted by independent, trusted third parties of their choice).

E2E-V elections can utilize paper ballots or operate purely electronically, the latter offering a means of auditing elections that support voters with visual and/or motor-skill limitations.

Risk-limiting auditing and public auditing using E2E-verifiability may address some security risks associated with tampering. The techniques can be used in combination.

RECOMMENDATIONS

5.5 Each state should require a comprehensive system of post-election audits of processes and outcomes. These audits should be conducted by election officials in a transparent manner, with as much observation by the public as is feasible, up to limits imposed to ensure voter privacy.

5.6 Jurisdictions should conduct audits of voting technology and processes (for voter registration, ballot preparation, voting, election reporting, etc.) after each election. Privacy-protected audit data should be made publicly available to permit others to replicate audit results.

5.7 Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast.

5.8 States should mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots.[25] States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.

5.9 State and local jurisdictions purchasing election systems should ensure that the systems will support cost-effective risk-limiting audits.

5.10 State and local jurisdictions should conduct and assess pilots of end-to-end-verifiable election systems in elections using paper ballots.

INTERNET VOTING

Overview and Analysis

As more aspects of people's lives move online, it is natural to ask whether the future of voting will also be online. Many people are familiar with and comfortable with the Internet as a tool and conduct what might be considered high-risk transactions (e.g., banking, e-commerce, the transmission of medical records, etc.) online. Internet voting has the potential to increase convenience and perhaps increase participation.[26] With Internet voting, all ballots would be marked using software run on a special voting station or on a voter's own smartphone, tablet, laptop, or desktop computer. Completed ballots would then be transmitted electronically to be tabulated. Although Internet voting offers convenience, it introduces new risks with regard to the integrity and confidentiality of votes as well as the potential for cyberattacks that could make it difficult or impossible for voters to cast their ballots within

[25] Risk-limiting audits examine individual randomly selected paper ballots until there is sufficient statistical assurance to demonstrate that the chance that an incorrect reported outcome escaping detection and correction is less than a predetermined risk limit.

[26] Katherine Stewart and Jirka Taylor, analysts for the RAND Corporation, recently concluded that "the observed impact of online voting on voting behaviour to date has been varied. In some cases, it has led to an initial increase in voter turnout. But whether this leads to a long-term trend of sustained voter engagement, particularly among younger people, remains unclear." Citing numerous sources, Stewart and Taylor suggest that online voting "may not be the 'silver bullet' in addressing the wider problem of voter disengagement." See https://www.rand.org/blog/2018/03/online-voting-the-solution-to-declining-political-engagement.html?adbid=986626411103379461&adbpl=tw&adbpr=22545453&adbsc=social_20180418_2261001.

the voting period. Furthermore, the casting of a ballot is an anonymous one-time event. This scenario makes it difficult to identify and correct a miscast vote.

Insecure Internet voting is possible now, but the risks currently associated with Internet voting are more significant than the benefits. Secure Internet voting will likely not be feasible in the near future.

Many vendors, however, currently offer Internet voting systems. Private elections (e.g., corporate shareholder elections) are often conducted primarily over the Internet. Some public elections have allowed Internet voting as an option or even used the Internet as the sole medium for casting votes. As discussed on page 68, voting by fax is sometimes allowed for absentee voters, and completed ballots are sometimes accepted as email attachments.

To ensure secure Internet voting, voters must be supplied with suitable digital credentials that allow them to prove their identity when voting online. Such credentials are supplied to all citizens in some nations (e.g., Estonia). These credentials allow individuals to access a variety of government services. Estonia has extended these services to voting.[27] Neither the U.S. federal government nor the states seem likely to supply universal digital credentials in the near future.[28] If voting is the only purpose for which these credentials are used, voters might easily surrender their credentials to others. Simple PINs and passwords are inadequate for secure voting, and standard email is an inappropriate medium for distributing strong credentials or transmitting marked ballots.[29]

[27] Digital credentials may be vulnerable to hacking. In 2017, Estonia suspended the use of its identity smartcards in response to the discovery of a wide-ranging security flaw. More than 750,000 ID cards were affected. See, e.g., "Estonia Has Frozen Its Popular E-Residency ID Cards Because of a Massive Security Flaw," *Business Insider*, November 6, 2017, available at: http://www.businessinsider.com/estonia-freeze-e-residency-id-cards-id-theft-2017-11.

[28] The federal government does provide Common Access Cards (CACs). CACs are "'smart card[s]' about the size of a credit card." They are "standard identification for active duty uniformed Service personnel, Selected Reserve, DoD [U.S. Department of Defense] civilian employees, and eligible contractor personnel . . . [and] the principal card used to enable physical access to buildings and controlled spaces, and" provide "access to DoD computer network and systems." See http://www.cac.mil/common-access-card/.

[29] See, e.g., U.S. Vote Foundation, "The Future of Voting: End-to-end Verifiable Internet Voting—Specifications and Feasibility Study," July 2015, p. 112, available at: https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf.

Obstacles to Internet Voting

Many concerns must be addressed before secure Internet voting would be feasible.[30]

Malware

The malware threat present whenever software is used is amplified in the case of Internet voting when voters use personal devices. Such devices may be less well tended and protected than the dedicated election equipment maintained by election officials.

Denial-of-service Attacks

While denial-of-service (DoS) is a risk in any voting medium, it is a mainstay of today's Internet. Many vendors provide services that can mitigate, but not eliminate, these attacks. Unfortunately, the mitigations usually require full decryption of all transmitted data, and these services are performed on systems that are shared with numerous third parties.

Related Technologies

Several technologies are directly relevant to Internet voting.

Secure Channel Technologies

Email is an Internet technology. Most email does not utilize the secure channel technologies commonly used for applications such as online banking and shopping. This makes email voting more vulnerable than many other forms of Internet voting.

Most fax transmissions travel, at least in part, over the Internet and therefore should also be regarded as a form of Internet voting with all of the added risks.

Blockchains

Blockchains are a technology meant to achieve an unalterable, decentralized, public, append-only log of transactions, without any single authority in a position to change the log. In an election context, the "transactions" would be the casting of ballots. A blockchain could therefore act as a virtual electronic ballot box. Blockchains may be managed publicly or by a

[30] In addition to the concerns described below, server-side break-ins (demonstrated against the Washington, DC, system in 2010), man-in-the-middle attacks (demonstrated against New South Wales in 2015), and authentication technology vulnerabilities (discovered in Estonia's system in 2017) represent other obstacles that must be addressed before Internet voting would be feasible.

restricted set of managers.[31] Several companies provide, or are attempting to build, voting systems around blockchains.[32]

While the notion of using a blockchain as an immutable ballot box may seem promising, blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities. In particular, if malware on a voter's device alters a vote before it ever reaches a blockchain, the immutability of the blockchain fails to provide the desired integrity, and the voter may never know of the alteration.

Blockchains are decentralized, but elections are inherently centralized. Although blockchains can be effective for decentralized applications, public elections are inherently centralized—requiring election administrators define the contents of ballots, identify the list of eligible voters, and establish the duration of voting. They are responsible for resolving balloting issues, managing vote tabulation, and announcing results. Secure voting requires that these operations be performed verifiably, not that they be performed in a decentralized manner.

While it is true that blockchains offer observability and immutability, in a centralized election scenario, observability and immutability may be achieved more simply by other means. Election officials need only, for example, post digitally signed versions of relevant election-related reports for public observation and download.

Ballots stored on a blockchain are electronic. While paper ballots are directly verifiable by voters, electronic ballots (i.e., ballots on a blockchain) can be more difficult to verify. Software is required to examine postings on blockchain. If such software is corrupted, then verifiability may be illusory. Software independence is not, therefore, achieved through posting ballots on a blockchain: as ballots are represented electronically, software independence may be more difficult to achieve.

The blockchain abstraction, once implemented, provides added points of attack for malicious actors. For example, blockchain "miners" or "stakeholders" (those who add items to the blockchain) have discretionary control over what items are added. Miners/stakeholders might collude to suppress votes from certain populations or regions. Furthermore, blockchain protocols generally yield results that are a consensus of the miners/stakeholders. This consensus may not represent the consensus of the voting public. Miners/stakeholders with sufficient power might also cause confusion and uncertainty about the state of a blockchain by raising doubts about whether a consensus has been reached.

[31] Blockchains managed by a restricted set of managers are referred to as *provisioned blockchains*.

[32] Voatz, Inc. and Votem are two such companies.

Blockchains do not provide the anonymity often ascribed to them.[33] In the particular context of elections, voters need to be authorized as eligible to vote and as not having cast more than one ballot in the particular election. Blockchains do not offer means for providing the necessary authorization.

Blockchains do not provide ballot secrecy. If a blockchain is used, then cast ballots must be encrypted or otherwise anonymized to prevent coercion andvote-selling. While E2E-V voting methods may provide the necessary cryptographic tools for this, ordinary blockchain methods do not.

It may be possible to employ blockchains within an election system by addressing the security issues associated with blockchains through the use of additional mechanisms (such as, for example, those provided by E2E-verifiability), but the credit for addressing such problems would lie with the additional mechanisms, not with the use of blockchains.

End-to-end-verifiable Systems

End-to-end-verifiable (E2E-V) technologies can be used in a variety of voting scenarios.

In its 2015 report, the U.S. Vote Foundation asserted that any possible future Internet voting system should utilize E2E-verification, but the report stated that this should not even be attempted before greater experience has been garnered with E2E-V systems deployed and used within in-person voting scenarios.[34]

E2E-V voting mitigates some of the vulnerabilities in Internet voting. However, advances in prevention of malware and DoS attacks need to be realized before *any* Internet voting should be undertaken in public elections—even if E2E-V.

[33] A July 13, 2018 federal indictment of twelve Russian operatives, for instance, describes in detail how the operatives were traced and identified through their use of the cryptocurrency bitcoin and its associated blockchain ledger. Count Ten of the indictment (Conspiracy to Launder Money) details how "the Conspirators" used bitcoin and its blockchain ledger in an attempt to "obscure their identities and their links to Russia and the Russian government" and how their use of bitcoin, despite the "perceived anonymity" of blockchains, was then exploited by investigators to identify the operatives. See *United States of America vs. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev*, Case 1:18-cr-00215-ABJ (2018), pp. 21-22, available at: https://www.justice.gov/file/1080281.

[34] "The Future of Voting: End-to-end Verifiable Internet Voting—Specifications and Feasibility Study," p. v.

Findings

All Internet voting schemes (including those that are E2E-V) are vulnerable to DoS attacks.

The Internet is not currently a suitable medium for the transmission of marked ballots, as Internet-based voting systems in which votes are cast on remote computers or other electronic devices and submitted electronically cannot be made adequately secure today.

E2E-verifiability may mitigate many of the threats associated with Internet voting.

Conducting secure and credible Internet elections will require substantial scientific advances.

The use of blockchains in an election scenario would do little to address the major security requirements of voting, such as voter verifiability. The security contributions offered by blockchains are better obtained by other means. In the particular case of Internet voting, blockchain methods do not redress the security issues associated with Internet voting.

RECOMMENDATIONS

5.11 At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.[35,36] Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.[37]

5.12 U.S. Election Assistance Commission standards and state laws should be revised to support pilot programs to explore and validate new election technologies and practices. Election officials are encouraged to seek expert and public comment on proposed new election technology before it is piloted.

[35] Inclusive of transmission via email or fax or via phone lines.

[36] The Internet is an acceptable medium for the transmission of unmarked ballots to voters so long as voter privacy is maintained and the integrity of the received ballot is protected.

[37] If secure Internet voting becomes feasible and is adopted, alternative ballot-casting options should be made available to those individuals who do not have sufficient access to the Internet.