No Simple Answers

A Primer on Ballot Marking Device Security

July 2022

CENTER FOR
DEMOCRACY
& TECHNOLOGY

CENTER FOR
DEMOCRACY
& TECHNOLOGY

The Center for Democracy & Technology (CDT) is a 25-year-old 501(c)3 nonpartisan nonprofit organization working to promote democratic values by shaping technology policy and architecture. The organisation is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

No Simple Answers

A Primer on Ballot Marking Device Security

Author

William T. Adler

With Contributions by

Allison McDonald, Elissa M. Redmiles, Elizabeth Seeger, Madeliene Dwyer, Samir Jain, and Tim Hoagland.

Acknowledgements

We thank Matt Bernhard, Mallory Knodel, and Mark Lindeman for their feedback and suggestions.

Footnotes in this report include original links as well as links archived and shortened by the Perma.cc service. The Perma.cc links also contain information on the date of retrieval and archive.

Source of QR code in cover illustration:

Bobmath and authors of en:QR code, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons.

Contents

Contents (cont.)

Introduction

The 2020 election and its aftermath was marked by conspiracy theories and disinformation about the machinery of the U.S. election system – the rules and mechanisms for registering and authenticating voters, collecting and counting votes, reporting those votes to Congress, and so on. A subset of those conspiracy theories focused on the literal election machinery – the computerized systems used for casting and counting ballots.

Legitimate concerns about BMD security can be hard to distinguish from outlandish claims about election machinery.

President Trump and his allies focused especially intensely[1] on discrediting and attempting to overturn the results in the state of Georgia, which President Biden won by a narrow margin. One year prior, under court order,[2] Georgia had replaced its paperless voting machines with touchscreen computers that print out a paper ballot – called ballot marking devices (BMDs) – for use by every in-person voter.[3] After the 2020 election, Georgia election officials countered an array of mis- and disinformation about the new voting machines, such as the allegation that the machines were somehow modified to "flip" Trump votes to Biden votes.[4]

BMDs are widely used in U.S. elections[5] and come with several benefits for election officials and voters. Because of their accessibility features – for example, allowing users to increase the displayed font size, use an auditory or sip-

[1] Gardner, A. (2021, March 11). Trump pressured a Georgia elections investigator in a separate call legal experts say could amount to obstruction. *Washington Post*. [perma.cc/4XZM-H3KZ]

[2] Greenhalgh, S. & Stark, P. (2022, March 4). Setting the record straight on the security review in the Georgia voting machine lawsuit. *Election Law Blog*. [perma.cc/V2J7-CYC6]

[3] Verified Voting. (n.d.). The Verifier — Election Day Equipment in Georgia — November 2020. [perma.cc/87QY-DU6C]

[4] Wickert, D. (2021, December 30). Five fraud claims: What investigators found. *Atlanta Journal-Constitution*. [perma.cc/2WCJ-XMBN]

[5] Verified Voting estimates that 20.8% of registered voters in 2022 live in jurisdictions where all voters will use BMDs if they vote in-person on Election Day. Most other voters will have the option of using a BMD if they choose; they are available as an option in most jurisdictions. Verified Voting. (n.d). The Verifier — Election Day Equipment — November 2022. [perma.cc/FU9P-WKAW]

and-puff interface, or change the displayed language – they enable voters to vote independently and privately, when they might otherwise be unable to do so.[6] They also prevent certain mistakes that could cause a ballot to be uncounted or counted incorrectly, like stray pen marks and overvoting (i.e., voting for too many candidates in a contest).

However, BMDs have been generally criticized as posing serious security risks to elections.[7] Georgia's BMDs have specifically been the focus of recent investigation from security researchers. A report conducted by security researcher J. Alex Halderman, which is currently under seal, reportedly indicates specific vulnerabilities in these machines.[8] In June 2022, the federal Cybersecurity and Infrastructure Agency (CISA) released an advisory summarizing these vulnerabilities.[9]

Legitimate concerns about BMD security, however, can be hard to distinguish from outlandish claims about election machinery. BMDs are often the focus of viral misinformation[10] and lawsuits[11] that may be intended to undermine trust in election systems. This primer on BMD security outlines some of the key questions that are frequently raised about the security of BMDs, and makes recommendations for protecting elections in which BMDs are used. BMDs present certain security risks, but some of those risks can be mitigated through the best practices set forth below.

BMDs are likely to be an important part of election infrastructure in the U.S. for the foreseeable future. Accordingly, we also look ahead to how BMD security might be enhanced in the long term, particularly as vendors start implementing the provisions in the U.S. Election Assistance Commission's recent update to the Voluntary Voting Systems Guidelines (VVSG 2.0) – the first major update in 15 years.

[6] Private and independent voting is a requirement of the federal Help America Vote Act (2002). Some voter advocacy organizations advocate for BMDs as a way to meet these requirements. Disability Rights Florida. (n.d.) Using Paper Ballots. [perma.cc/A5XN-AZWY]

[7] Appel, A.W., DeMillo, R.A., & Stark, P.B. (2020). Ballot-marking devices cannot ensure the will of the voters. *Election Law Journal: Rules, Politics, and Policy*. [perma.cc/AB7D-32BK]

[8] Pagliery, J. & Vavra, S. (2021, August 13). Judge Seals Report on Voting Machine Vulnerability. *Daily Beast*. [perma.cc/J6A3-87JM]

[9] U.S. Cybersecurity and Infrastructure Security Agency. (2022, June 3). Vulnerabilities Affecting Dominion Voting Systems ImageCast X. [perma.cc/2X7T-8ZYE]

[10] Woolverton, P. (2021, January 5). Fact check: QR codes on Georgia ballots record votes as cast. *USA Today*. [perma.cc/K93B-N7Z2]

[11] Dunlap, S. (2021, August 25). Suit backed by Georgia lawmaker challenges state's ballot barcode system. *Georgia Recorder*. [perma.cc/C8YW-N6GQ]

Background

Components of electronic voting systems

Electronic voting systems gained prevalence after the passage of the Help America Vote Act of 2002, which provided funding to states to replace outdated and malfunctioning voting equipment, like punch-card and lever machines.[12] Today, electronic devices may be used for casting votes, tabulating votes, or both. Devices are used for other important functions too, such as registering voters and checking voters in, but this report only focuses on those devices used for casting and tabulating votes.

***

Ballot marking devices

Ballot marking devices (BMDs) are special-purpose computers that voters use to make and print out their selections (Fig. 1). VVSG 2.0 defines a BMD[13] as a device that:

- permits contest options to be selected and reviewed on an electronic interface;
- produces a human-readable paper ballot; and
- does not make any other lasting record of the voter's selections.

The ballot produced by a BMD may appear similar to a hand-marked paper ballot (HMPB): a ballot showing every contest option, with filled bubbles next to the voter's selections (Fig. 4). Alternatively, a BMD may produce a "summary ballot," printing only the voter's selections (Fig. 3). The BMD may additionally print voter selections encoded in a barcode or quick-response (QR) code, a two-dimensional barcode. Barcodes are used because scanners can interpret them quickly and reliably.[14]

***

[12] U.S. Election Assistance Commission. (n.d.). Help America Vote Act. [perma.cc/3KF5-MJ35]

[13] U.S. Election Assistance Commission. (2021, February 10). Requirements for the Voluntary Voting System Guidelines 2.0, p. 266. [perma.cc/8JA9-BH5R]

[14] VotingWorks. (n.d.). Barcodes Are a Distraction: Focus on Audits. [perma.cc/AT5B-APU2]

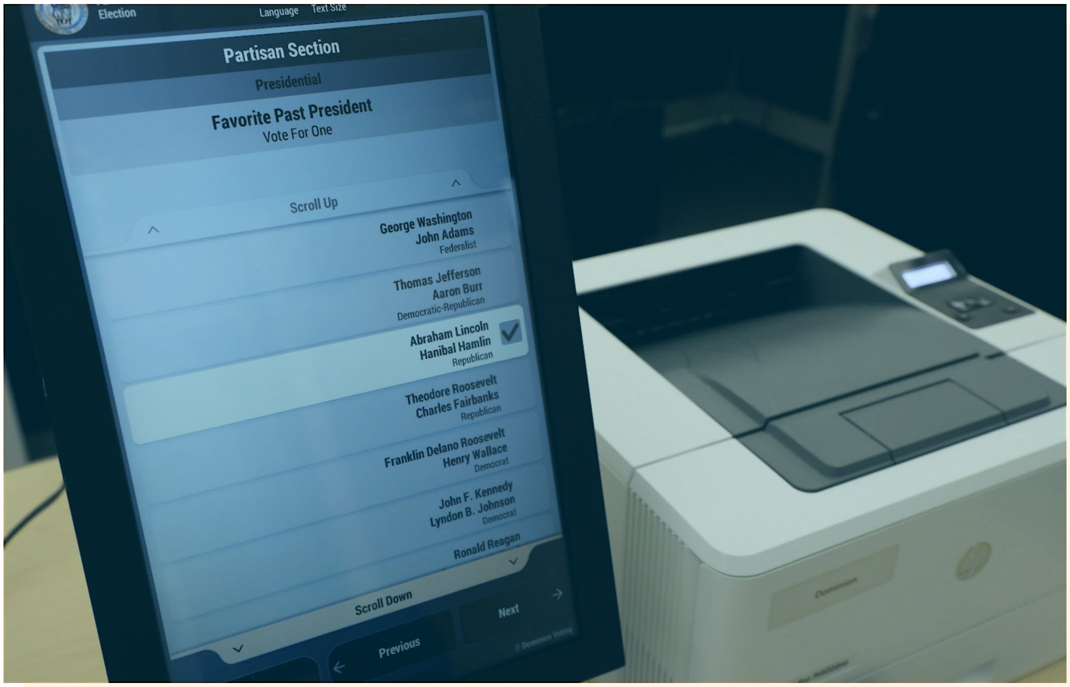


Figure 1. A Dominion ImageCast X BMD configured to print out ballots on a laser printer. (Source: Michigan Department of State / YouTube)[15]

Optical scanners

Optical scanners tabulate paper ballots, which may be marked by hand or with a BMD. Ballots may be tabulated when the voter feeds the ballot into the scanner at the polling place (Fig. 2) or, alternatively, in bulk at a central location. An optical scanner is loaded with information about the ballots (i.e., a list of contests and candidates, the format of the paper ballots, etc.) before ballots are inserted, so that it knows how to interpret the ballots. As ballots are inserted, the scanner will read selections either by scanning a machine-readable record of the voter's selections (e.g., a barcode or a set of barcodes) or by using the ballot configuration to identify how marks (e.g., filled bubbles) on the ballot correspond to voter selections.

***

[15] Michigan Department of State / Secretary of State. (2020, November 2). Voting with the Dominion ImageCast X (ICX). *YouTube*. [perma.cc/ZKK3-3QBW]

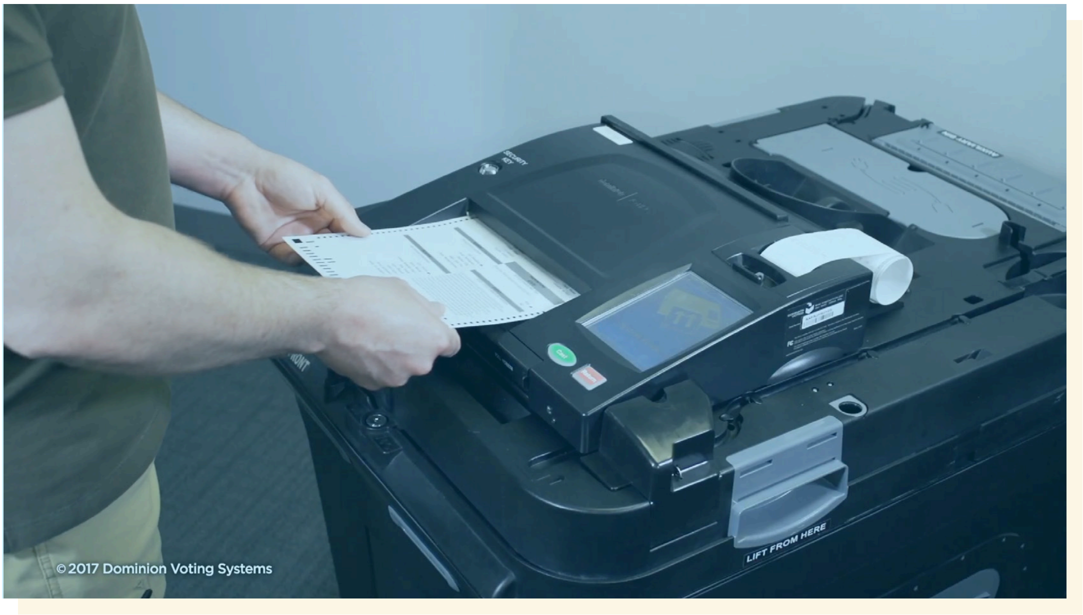


Figure 2. A voter inserts a ballot into the Dominion ImageCast Precinct, which scans and tabulates the ballot. (Source: Dominion Voting Systems / YouTube)[16]

Direct-recording electronic voting machines

A direct-recording electronic (DRE) voting machine allows a voter to make their selections on a screen. However, instead of producing a paper ballot that the voter then feeds into an optical scanner for tabulation, it tabulates the voter's choice directly, storing the result in memory. Some DREs are equipped with voter-verified paper audit trail (VVPAT) attachments that print out a paper receipt of the voter's choice and display it to the voter from behind a transparent window.[17]

***

Software independence

To ensure the security of elections that rely on computers, election security experts have advocated for systems to be "software independent."[18] Software independence is now a requirement for voting systems to be certified to VVSG 2.0, where it is defined as a characteristic of a voting system for which "a previously undetected change or fault in software cannot cause an undetectable change or

[16] Commonwealth Media Services, Department of General Services, Commonwealth of Pennsylvania. (2019, May 15). Dominion ICP Step 2 – Marking and Casting the Ballot. [perma.cc/53KG-DMBB]

[17] Verified Voting. (n.d.). AccuVote TSX. [perma.cc/G2R7-CB86]

[18] Rivest, R.L. (2008, August 6). On the notion of "software independence" in voting systems. *Philosophical Transactions of the Royal Society A*. [perma.cc/B97S-PUTX]

error in election outcome."[19] In other words, if a voting system is software independent, it is possible to audit and verify the election outcome without having to trust that the software is correct.

Software independence can be achieved when a system produces a voter-verifiable paper record[20] that cannot be undetectably altered by the voting system's software after voter review. This way, if a software error occurs (e.g., if an optical scanner tabulates ballots incorrectly), the result can still be determined by a full or partial hand tally of voter-verified ballots. A BMD may be part of a software independent voting system: by definition, it produces a voter-verifiable paper record.[21]

Election security experts have advocated for systems to be "software independent."

DREs often do not produce a paper record at all. This means that, after an election, there is no way to verify that the records produced by a DRE match voters' choices. Because an undetected change in the software could therefore alter vote records without leaving a trace, paperless DREs are not software independent. DREs that print out a VVPAT may be software independent;[22] unfortunately, though, these VVPAT attachments have been roundly criticized by election experts for usability and ballot secrecy concerns.[23] For these reasons, experts have strongly encouraged election administrators to abandon DREs in favor of a combination of HMPBs and BMDs.[24] Accordingly, DREs have fallen out of favor in the U.S. In 2006, 42.4% of voters lived in counties where all voters used DREs. In 2022, that number is expected to be just 8%.

[19] U.S. Election Assistance Commission. (2021, February 10). Requirements for the Voluntary Voting System Guidelines 2.0, p. 181. [perma.cc/9XAR-ZSL8]

[20] As of June 2019, all but 13 states had some requirement for voting systems to produce a paper trail of ballots (though not all requirements stipulate that the paper trail should be *voter verifiable*). National Conference of State Legislatures. (2019, June 27). Voting System Paper Trail Requirements. [perma.cc/A88J-53SW]

[21] However, there are cases in which a BMD may be designed in a way that is not software independent. For instance, if a BMD is capable of printing on the ballot selection area, altering the ballot after voter verification (thereby undetectably altering the record), the system would not be software independent.

[22] Rivest, R. (2006, December 4). Software Independence and Encouraging Innovation in VVSG 2007: Presentation for the Technical Guidelines Development Committee, p. 23. [perma.cc/KS82-52EU]

[23] Verified Voting. (2022, February 10). Letter to Indiana Senate Elections Committee opposing the use of voter-verified paper audit trails in HB 1116 instead of paper ballots. [perma.cc/F8RR-8LRL]
Goggin, S.N. & Byrne, M.D. (2007). An examination of the auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots. *USENIX*. Appel, A. (2018, October 19). Continuous-roll VVPAT under glass: an idea whose time has passed. *Freedom to Tinker*.

[24] National Academies of Sciences, Engineering, and Medicine (2018). Securing the Vote: Protecting American Democracy. *The National Academies Press*. [perma.cc/8A6S-XPZE]

Key Questions About Ballot Marking Devices

Given the critical role that BMDs have – and will likely continue to have – in U.S. elections, we present questions that journalists, election administrators, and members of the public may have concerning their potential failures, necessity, and usage.

***

How can BMDs fail?

Like any computer system, BMDs can fail in a number of ways[25] – they can have software bugs, they can have design flaws that lead to user error, or they can be manipulated by an attacker. While there is no evidence that such attacks have impacted a real election, security and voting researchers have demonstrated the feasibility of these attacks for years.[26] The attacks we discuss are therefore theoretical but possible.[27]

While there is no evidence that such attacks have impacted a real election, security and voting researchers have demonstrated the feasibility of these attacks for years. The attacks we discuss are therefore theoretical but possible.

A compromised BMD could be modified to print a vote for a candidate that is different from the one the voter selected on the screen. While voters using HMPBs may mistakenly vote for a candidate they did not intend to or neglect to vote in a contest (particularly if the ballot is poorly designed),[28] a hacked BMD could corrupt voter selections systematically, such that a candidate favored by the hacker is more likely to win.

***

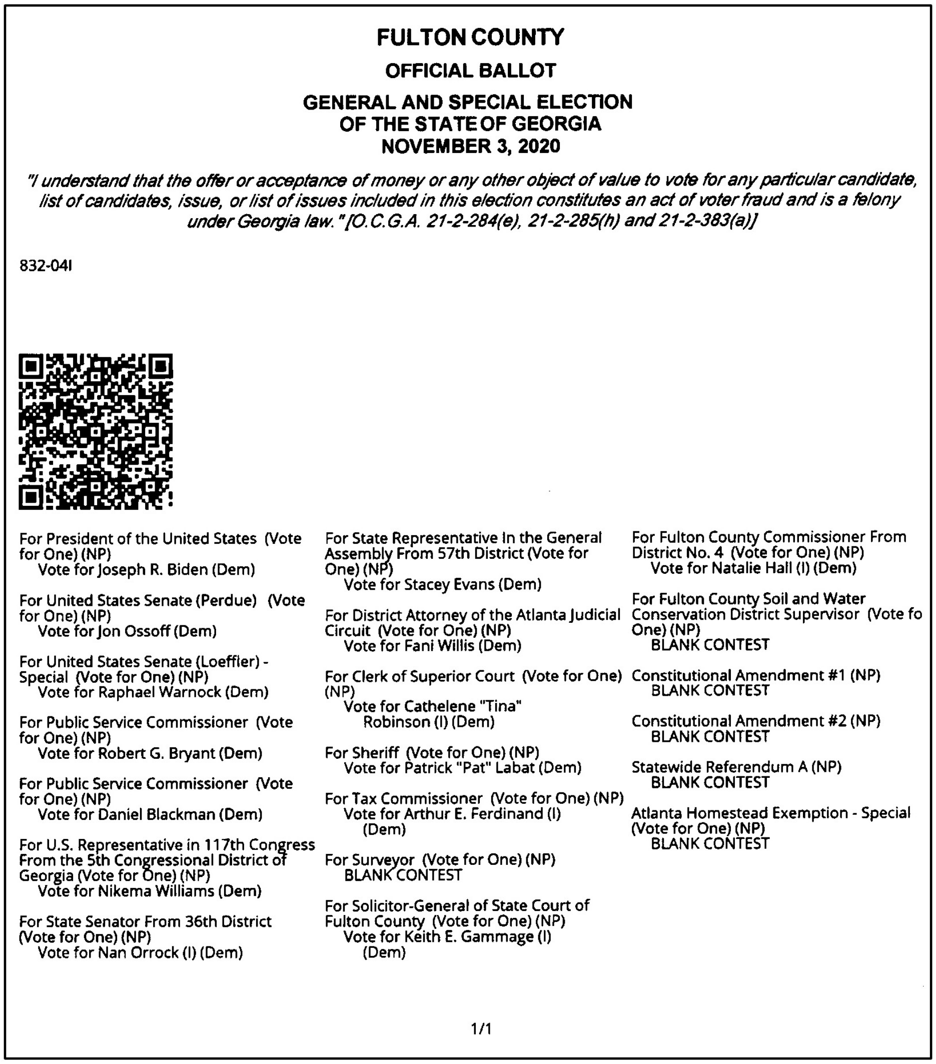
[25] Norden, L. (2010, September 13). Voting System Failures: A Database Solution. *Brennan Center for Justice*. [perma.cc/H8WE-U924]

[26] Appel, A.W., DeMillo, R.A., & Stark, P.B. (2020). Ballot-marking devices cannot ensure the will of the voters. *Election Law Journal: Rules, Politics, and Policy*. [perma.cc/AB7D-32BK]

[27] We do not discuss here the technical requirements to carry out an attack, nor reason about the likelihood of an attack being successful.

[28] McCadney, A.C. & Norden, L. (2020, February 3). Common Ballot Design Flaws and How to Fix Them. *Brennan Center for Justice*. [perma.cc/24ED-PJXU]

Inconsistent barcode attack



FULTON COUNTY

OFFICIAL BALLOT

GENERAL AND SPECIAL ELECTION
OF THE STATE OF GEORGIA
NOVEMBER 3, 2020

"I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law." [O.C.G.A. 21-2-284(e), 21-2-285(h) and 21-2-383(a)]

832-04I

For President of the United States (Vote for One) (NP)
Vote for Joseph R. Biden (Dem)

For United States Senate (Perdue) (Vote for One) (NP)
Vote for Jon Ossoff (Dem)

For United States Senate (Loeffler) - Special (Vote for One) (NP)
Vote for Raphael Warnock (Dem)

For Public Service Commissioner (Vote for One) (NP)
Vote for Robert G. Bryant (Dem)

For Public Service Commissioner (Vote for One) (NP)
Vote for Daniel Blackman (Dem)

For U.S. Representative in 117th Congress From the 5th Congressional District of Georgia (Vote for One) (NP)
Vote for Nikema Williams (Dem)

For State Senator From 36th District (Vote for One) (NP)
Vote for Nan Orrock (I) (Dem)

For State Representative In the General Assembly From 57th District (Vote for One) (NP)
Vote for Stacey Evans (Dem)

For District Attorney of the Atlanta Judicial Circuit (Vote for One) (NP)
Vote for Fani Willis (Dem)

For Clerk of Superior Court (Vote for One) (NP)
Vote for Cathelene "Tina" Robinson (I) (Dem)

For Sheriff (Vote for One) (NP)
Vote for Patrick "Pat" Labat (Dem)

For Tax Commissioner (Vote for One) (NP)
Vote for Arthur E. Ferdinand (I) (Dem)

For Surveyor (Vote for One) (NP)
BLANK CONTEST

For Solicitor-General of State Court of Fulton County (Vote for One) (NP)
Vote for Keith E. Gammage (I) (Dem)

For Fulton County Commissioner From District No. 4 (Vote for One) (NP)
Vote for Natalie Hall (I) (Dem)

For Fulton County Soil and Water Conservation District Supervisor (Vote fo One) (NP)
BLANK CONTEST

Constitutional Amendment #1 (NP)
BLANK CONTEST

Constitutional Amendment #2 (NP)
BLANK CONTEST

Statewide Referendum A (NP)
BLANK CONTEST

Atlanta Homestead Exemption - Special (Vote for One) (NP)
BLANK CONTEST

1/1

Figure 3. The Dominion ImageCast X BMD prints a summary ballot, printing voter selections in text and encoding them in a QR code. (Source: Mark Lindeman)

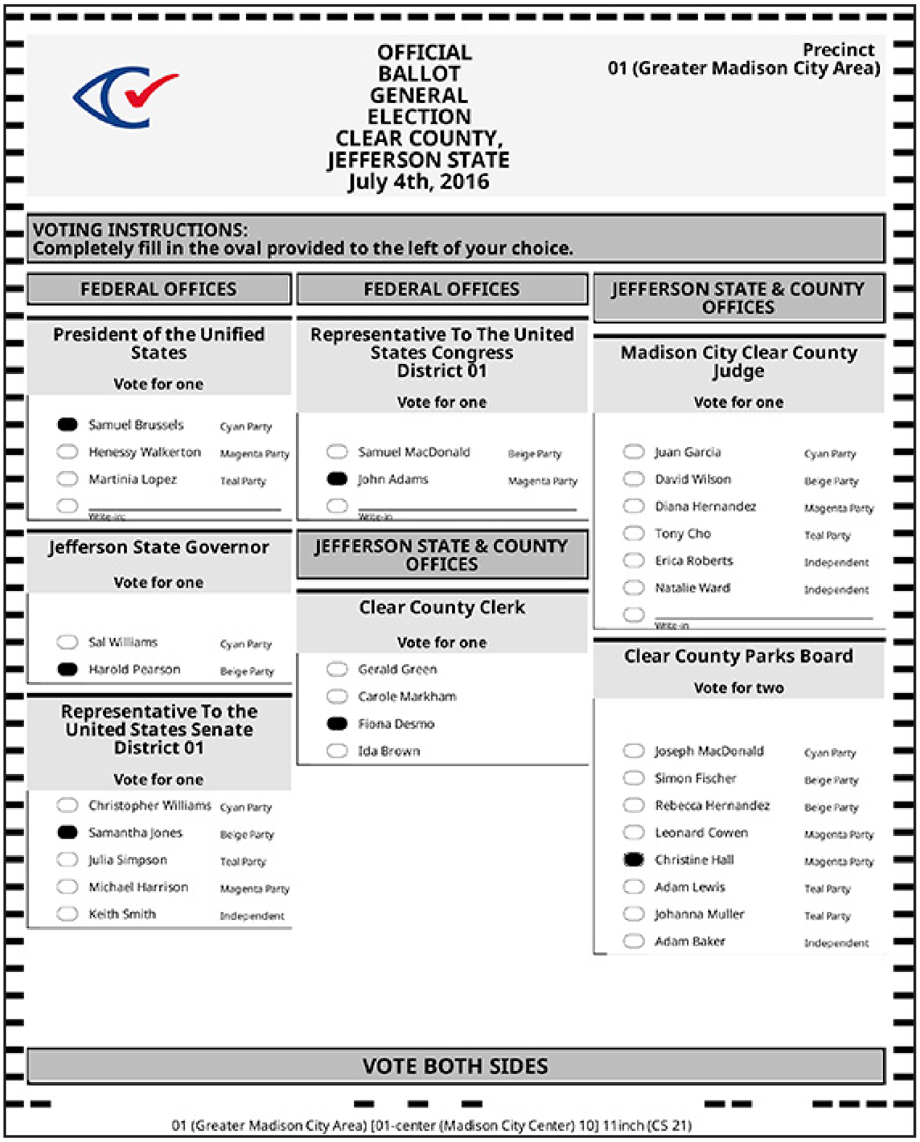
One option for an attacker would be to modify the BMD to print an incorrect vote in a way that is undetectable by the voter. For example, if the BMD (e.g., the Dominion ImageCast X, Fig. 3) prints a ballot that encodes selections in a barcode, the BMD could modify the choices encoded in the barcode but still print the voters' intended choices in the human-readable text. Wallach (2019) has called this the "inconsistent barcode attack."[29] This attack would be nearly impossible to detect during an election because the ballots would appear correct to the voter. However, a risk-limiting audit (RLA) would have a high likelihood of mitigating the attack, correcting an incorrect

[29] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

election outcome by counting only the human-readable portion of the ballots.[30]

***

Text swap attack



Precinct
01 (Greater Madison City Area)

OFFICIAL
BALLOT
GENERAL
ELECTION
CLEAR COUNTY,
JEFFERSON STATE
July 4th, 2016

VOTING INSTRUCTIONS:
Completely fill in the oval provided to the left of your choice.

FEDERAL OFFICES

President of the Unified States
Vote for one

● Samuel Brussels Cyan Party
○ Henessy Walkerton Magenta Party
○ Martinia Lopez Teal Party
○ Write-in

Jefferson State Governor
Vote for one

○ Sal Williams Cyan Party
● Harold Pearson Beige Party

Representative To the United States Senate District 01
Vote for one

○ Christopher Williams Cyan Party
● Samantha Jones Beige Party
○ Julia Simpson Teal Party
○ Michael Harrison Magenta Party
○ Keith Smith Independent

FEDERAL OFFICES

Representative To The United States Congress District 01
Vote for one

○ Samuel MacDonald Beige Party
● John Adams Magenta Party
○ Write-in

JEFFERSON STATE & COUNTY OFFICES

Clear County Clerk
Vote for one

○ Gerald Green
○ Carole Markham
● Fiona Desmo
○ Ida Brown

JEFFERSON STATE & COUNTY OFFICES

Madison City Clear County Judge
Vote for one

○ Juan Garcia Cyan Party
○ David Wilson Beige Party
○ Diana Hernandez Magenta Party
○ Tony Cho Teal Party
○ Erica Roberts Independent
○ Natalie Ward Independent
○ Write-in

Clear County Parks Board
Vote for two

○ Joseph MacDonald Cyan Party
○ Simon Fischer Beige Party
○ Rebecca Hernandez Beige Party
○ Leonard Cowen Magenta Party
● Christine Hall Magenta Party
○ Adam Lewis Teal Party
○ Johanna Muller Teal Party
○ Adam Baker Independent

VOTE BOTH SIDES

01 (Greater Madison City Area) [01-center (Madison City Center) 10] 11inch (CS 21)

Figure 4. The Clear Ballot ClearAccess BMD prints a "bubble ballot" that looks similar to a HMPB, encoding voter selections in the position of the filled bubbles. (Source: Clear Ballot)[31]

[30] Furthermore, a post-election ballot-level comparison audit might not only correct the election outcome, but uncover the attack. A ballot-level comparison audit is a type of RLA that compares the human-readable portion of a ballot to how it was interpreted by the tabulator. Other types of RLAs compare hand and machine vote tallies but do not examine individual ballots. Verified Voting. (n.d.) Risk-Limiting Audit Methods. [perma.cc/E4AN-Z33H]

[31] Clear Ballot. (n.d.). ClearAccess. [perma.cc/Y6WX-TMYV]

Instead of printing out ballots with barcodes, some BMDs print ballots with filled-in bubbles that appear similar to hand-marked paper ballots (Fig. 4).[32] When tabulating these bubble ballots, scanners interpret only the position of the filled bubbles, entirely ignoring the text next to the bubbles. In other words, as with ballots with barcodes, these ballots also contain both a human-readable record (the text next to the filled bubbles) and a machine-readable record (the positions of the filled bubbles). A hacked BMD that prints bubble ballots might therefore swap the position of the text and the position of the filled bubble (Fig. 5). This "text swap attack," while perhaps easier to detect,[33] is essentially the same as the inconsistent barcode attack—an attack on the BMD that exploits how the scanner will interpret the ballot. As with the inconsistent barcode attack, an RLA is the best protection against this attack.

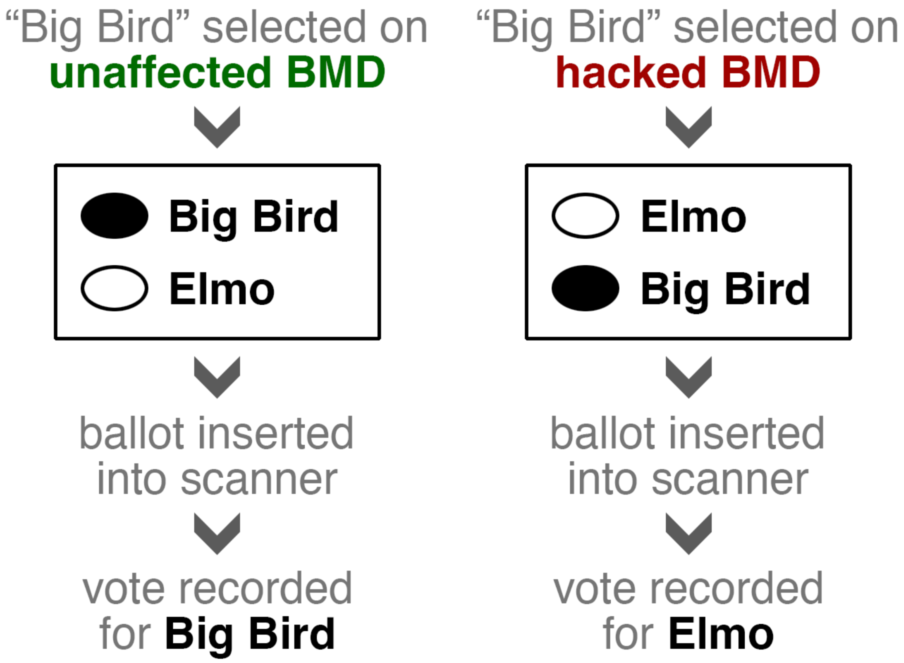


Figure 5. Consider a voter who intends to vote for Big Bird on a BMD that prints bubble ballots. A hacked BMD (right) might switch the position of the filled bubble and the text. To the voter, the ballot would look correct. But the ballot scanner, which has been programmed to interpret a lower filled bubble as a vote for Elmo, would record a vote for Elmo.

[32] This ballot style may be preferable for a few reasons: it indicates non-selected choices; it increases privacy for BMD users by being harder to distinguish from HMPBs; it may benefit voter trust to not have a barcode on the ballot. Skoglund, K. (2021, August). Are Barcodes on Ballots Bad? *DEF CON 29 Voting Village*. [perma.cc/7MEU-DLLZ]

[33] For example, by a person comparing a sample ballot to a BMD-printed ballot.

***

Switched intent attack

A hacked BMD could also print the incorrect selections in the human-readable portion of the ballot, the part that the voter can review and verify. Wallach (2019) has called this the "switched intent attack."[34] If undetected by a voter, this would corrupt the voter's choice in a way that could be undetectable after the fact. The weakness of this attack is that voters could detect it. The critical role of voters in detecting such an attack raises the question of whether voters can and do verify their BMD-printed ballots for errors.

Multiple papers suggest that voters are capable of detecting if a BMD-printed ballot contains selections different from those made by the voter.[35] But the proportion of voters who do bother to verify their ballots is unclear – and is likely highly dependent on the instructions and support they receive.

Multiple papers suggest that voters are capable of detecting if a BMD-printed ballot contains selections different from those made by the voter. But the proportion of voters who do bother to verify their ballots is unclear.

In a poll of Georgia voters in the 2020 general election, 90% of respondents said that they reviewed their paper ballot before casting it.[36] But an observational study showed that only about half of these voters looked at their ballot for more than one second.[37] Another study had participants vote in a fake election on BMDs modified to introduce an error on each printed ballot. In the absence of instruction to verify their ballots, only about 40% of participants did so, and fewer than 10% of participants actually reported noticing that something was wrong with their ballot.[38]

[34] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

[35] Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K., & Halderman, J.A. (2020). Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *2020 IEEE Symposium on Security and Privacy*. [perma.cc/KDD8-F375]
Kortum, P., Byrne, M.D., Azubike, C.O., & Roty, L.E. (2022, April 20). Can Voters Detect Errors on Their Printed Ballots? Absolutely. *arXiv*. [perma.cc/RP43-9V77]
Kortum, P., Byrne, M.D., & Whitmore, J. (2020, March 10). Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't. *arXiv*. [perma.cc/ZY5B-RTPE]

[36] Center for Election Innovation & Research. (2021). POST-GENERAL ELECTION SURVEY OF VOTING MACHINE VOTERS. [perma.cc/S3TE-GDJD]

[37] Niesse, M. (2021, July 27). Under half of Georgia voters checked their paper ballots, study shows. *Atlanta Journal-Constitution*. [perma.cc/E6HD-SMVE]

[38] Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K., & Halderman, J.A. (2020). Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *2020 IEEE Symposium on Security and Privacy*. [perma.cc/KDD8-F375]

There may be interventions that increase the proportion of voters who notice a change, though, including making ballots more readable, having poll workers prompt voters to review their printed ballot, or creating dedicated "ballot verification stations" for voters.[39] Two of the above studies demonstrated that providing written or verbal instruction can substantially increase the number of voters who review their ballots and report errors.

***

Denial-of-service attack

A more straightforward attack could involve modifying BMDs to be slow or nonfunctional, denying machine availability to voters. This could create long wait times, disenfranchising discouraged voters. Such an attack would be particularly effective for jurisdictions that rely entirely on BMDs. As with the above attacks that involve flipping votes, a denial-of-service attack could easily be designed to have an impact on the outcome; by creating outages in areas likely to vote mostly for one party, an outcome could be tipped for the other party.[40]

***

Should we stop using BMDs?

The potential for attacks on BMDs might suggest that we should move away from them entirely. Indeed, electronic voting is not the global norm.[41] 143 countries do not use any form of electronic voting; of those, nine countries used and then abandoned electronic voting.[42]

However, removing BMDs in favor of HMPBs does not guarantee that election results cannot be tampered with. Optical scanners could also be modified to miscount the otherwise correctly completed ballots input into the scanner. Optical scanner attacks do not only affect ballots completed with a BMD; they may cause the scanner to misinterpret HMPBs as well.[43]

[39] Kortum, P., Byrne, M.D., Azubike, C.O., & Roty, L.E. (2022, April 20). Can Voters Detect Errors on Their Printed Ballots? Absolutely. *arXiv*. [perma.cc/RP43-9V77]

[40] Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y.A., Stark, P.B., Teague, V., Vora, P.L., & Wallach, D.S. (2017, August 4). Public Evidence from Secret Ballots , p. 6. *arXiv*. [perma.cc/J499-9Y4B]

[41] American elections are particularly complex by international standards, though. A relatively large number of elected offices, ballot initiatives, and voting rules can mean many different ballot styles within a jurisdiction—increasing the benefit of electronic voting machines that can offer a flexible and streamlined voting experience.

[42] International Institute for Democracy and Electoral Assistance. (n.d.) ICTs in Elections Database – E-voting. [perma.cc/93KB-3YTW]

[43] Relatedly, some in the U.S. have pushed for the elimination of optical scanners. However,

Second, and most importantly, BMDs enable voters with disabilities, such as visual or physical impairments, to privately and independently cast a ballot – a right protected by federal law.[44] The population of voters with disabilities is not small. Approximately 7.7 million Americans, or 2.4% of the population, have a visual disability.[45] In 2020, 26%[46] of disabled voters voted at their polling place on Election Day. Of those voters, 18%[47] reported difficulties voting, compared to 10% of in-person voters without disabilities.

Some experts currently recommend using HMPBs as the primary method of voting, while minimizing the use of BMDs, e.g., only for voters who require them for accessibility reasons.[48] But there are costs to this approach. In 2021, a coalition of disability rights organizations expressed concerns that severely limiting BMD usage risks creating a segregated voting system, wherein voters with disabilities are the only group who use a particular type of voting machine.[49] They argued that this would increase "the likelihood that poll workers will not be properly trained on the machine, the machines will not be properly maintained or set up for use, and if the only available BMD is not functioning, there is no alternative option for voters who need it." Moreover, if a BMD produces a ballot that appears different from HMPBs (as is the case with many BMDs), limiting the number of BMD users compromises ballot privacy – it might be possible to determine how people with disabilities voted by looking at the BMD-produced ballots.[50]

Some experts currently recommend using HMPBs as the primary method of voting, while minimizing the use of BMDs, e.g., only for voters who require them for accessibility reasons. But there are costs to this approach.

this would likely make vote-counting slower and less accurate. As with BMDs, strong post-election audit practices can mitigate the potential harms from attacks on optical scanners. Montellaro, Z. (2022, March 6). Trump backers push election change that would make counting slower, costlier and less accurate. *Politico*. [perma.cc/GRZ2-BU8S]

[44] U.S. Department of Justice. (2014, September). The Americans with Disabilities Act and Other Federal Laws Protecting the Rights of Voters with Disabilities: Federal Laws Protecting the Right to Vote. [perma.cc/7E7J-6H5T]

[45] National Federation of the Blind. (2019, January). Blindness Statistics. [perma.cc/9LNV-XBUL]

[46] Schur, L. & Kruse, D. (2021, July). Fact sheet: Disability and Voter Turnout in the 2020 Elections. [perma.cc/9DRR-7R5F]

[47] Schur, L. & Kruse, D. (2021, February 16). Disability and Voting Accessibility in the 2020 Elections: Final Report on Survey Results. [perma.cc/ML5E-NS8P]

[48] Appel, A.W., DeMillo, R.A., & Stark, P.B. (2020). Ballot-marking devices cannot ensure the will of the voters. *Election Law Journal: Rules, Politics, and Policy*. [perma.cc/AB7D-32BK]

[49] National Disability Rights Network. (2021, January 29). Disability Community Fears Paper Ballot Mandate Will Hurt Voters with Disabilities. [perma.cc/7FJE-3R9K]

[50] Lazar, J. (2019, December 3). Segregated Ballots for Voters with Disabilities? An Analysis of Policies and Use of the ExpressVote Ballot Marking Device. *Election Law Journal: Rules, Politics, and Policy*. [perma.cc/W9JS-HK3Y]

In recognition of these costs, other experts have recommended a balanced approach. Verified Voting, a group of election security experts, recommends that polling places offer both HMPBs and BMDs and attempt to ensure that a variety of voters use BMDs. It even suggests, for instance, "inviting every 20th voter to use a BMD." But it recommends against implementing BMDs for all in-person voters because, e.g., HMPBs are more voter-verifiable, cheaper, and less prone to failure.[51]

Ideally, voters with disabilities should be afforded the same security and privacy guarantees as voters using HMPBs. Germany aims to increase parity through "ballot paper templates," an overlay on the ballot that allows voters with visual disabilities to use their own assistive devices, or Braille, to read the ballot choices and hand-mark their own ballots.[52] This approach might work for voters with visual disabilities, but voters who cannot mark ballot papers manually may still require an assistant, which compromises voter privacy and independence. Moreover, ballot paper templates are likely infeasible in the U.S., where ballots come in many different styles and often contain a large number of contests, therefore necessitating many different kinds of cumbersome templates.

In the near term, jurisdictions that use both BMDs and HMPBs should ensure that poll workers are well-trained on BMD usage, and that the machines are well-maintained and usable.[53] Looking forward, vendors and election officials should increase voter equity by ensuring that all voters have equal opportunity to mark and verify[54] their paper ballots privately and independently.

***

[51] Verified Voting. (2019, November 21). Policy on Direct Recording Electronic Voting Machines and Ballot Marking Devices. [perma.cc/CYY9-M64E]

[52] Federal Returning Officer (Germany). (2019, April 29). 2019 European Election: information for blind and visually impaired voters and on polling station accessibility. [perma.cc/D6NP-EVDD]

[53] U.S. Election Assistance Commission. (2020, February 20). 2020 Elections Disability, Accessibility, and Security Forum (Transcript). [perma.cc/GVD2-HCDS]

[54] While visually impaired voters may be able to use a BMD to mark their ballot with an auditory interface, they may have a harder time verifying their printed ballot. They may be able to use an optical character recognition (OCR) app on their phone to read back the selections on a summary ballot. But what about for a BMD that prints out a full ballot with filled bubbles? To our knowledge, there is not yet an app that can indicate the selections next to filled bubbles. This is a gap that OCR app developers should consider filling.

Do barcodes on BMD-printed ballots introduce unique vulnerabilities?

In the “inconsistent barcode attack” described above, a malicious BMD accurately prints the voter’s intended choices in the human-readable portion of the ballot, while modifying the choices encoded in the barcode that will be scanned and counted.[55] Because humans cannot easily read and verify the barcode, the attack is essentially impossible to detect during an election, as a ballot will look correct even to a discerning voter. In response to these concerns, some election experts have discouraged the use of barcodes for vote tabulation.[56] In 2019, Colorado decided to remove QR codes from its ballots entirely, in favor of BMD-printed bubble ballots.[57]

However, eliminating barcodes does not entirely prevent a compromised BMD from printing a ballot that would be tabulated in a way inconsistent with a voter’s selections. For instance, BMDs that encode voter choice with filled bubbles instead of barcodes are still vulnerable to the “text swap attack” described above. Therefore, a BMD that encodes voter selections in a barcode is not necessarily more vulnerable than a BMD that encodes selections in the position of filled bubbles, which may be equally difficult for a voter to decode.[58]

Even HMPBs may be vulnerable to the text swap attack. Whether ballots are printed ahead of time or printed on demand,[59] it is possible that a voter could be handed a ballot that swaps the position of candidate names. A voter might then mark a bubble that a tabulator would interpret as a vote for their dispreferred choice. For example, in a precinct with a strong partisan lean, an attacker (e.g., a malicious ballot clerk) supplying ballots that swapped the names of two presidential candidates could reverse that precinct’s partisan lean – according to the tabulators.

To summarize, voters and tabulators interpret ballots differently – whether ballots are printed with a barcode, printed with filled bubbles, or even if marked by hand. So, relative to other common methods of voting, barcodes do not introduce categorically new vulnerabilities.

[55] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

[56] California Clean Money Campaign. (2020, September 23). Letter to California Secretary of State Alex Padilla. [perma.cc/D38D-UKE3]

[57] State of Colorado Department of State. (2019, September 16). Colorado Secretary of State Takes Action to Increase Cyber Security, Announces Initiative to Remove QR Codes from Ballots. [perma.cc/2NZA-NNDJ]

[58] VotingWorks. (n.d.). Barcodes Are a Distraction: Focus on Audits. [perma.cc/AT5B-APU2]

[59] National Conference of State Legislatures. (2021, November 2). Vote Centers. [perma.cc/A3JR-7TBL]

***

Can voters verify ballot barcodes?

One way to assuage concern about whether a BMD is encoding incorrect choices in the barcode is to allow voters to independently verify the data encoded in them. Barcodes and QR codes are standardized and easily interpreted by smartphone apps[60] – so, theoretically, voters can use such apps to easily scan and interpret such codes. But QR codes cannot encode an unlimited amount of information,[61] so BMDs may print QR codes that use short keys to indicate voter selections. For instance, a QR code on Los Angeles County's ballots may encode a voter's selection in a series of short keys: "4N/4E/H/J/3C/3K/35..."[62] A voter wanting to verify that their choices were properly encoded would need to look up the meaning of these keys. Los Angeles County posts these keys publicly.[63] This is laudable, and other jurisdictions should also enable voters to verify their QR codes. However, given the difficulties posed by getting voters to verify their BMD-printed ballots in the first place, it seems unlikely that voters would scan and cross-reference their QR codes in sufficient numbers to create a meaningful bulwark against barcode attacks.

***

How can we detect and mitigate BMD misbehavior?

There are a few ways to detect whether BMDs are malfunctioning – and to respond accordingly.

***

Pre-election auditing

Before an election takes place, election officials typically run machines through a battery of tests that evaluate the behavior of each machine, a process known as logic and accuracy testing. The processes vary by jurisdiction, but typically involve resetting the machines, running them through a mock election where the input votes are known, and

[60] International Organization for Standardization. (2015, February). QR Code bar code symbology specification. [perma.cc/ZKS8-DS7R]

[61] The amount of information that a QR code can contain depends on its resolution and the amount of data correction chosen. The QR code with the most resolution and the lowest amount of data correction can store 4,296 alphanumeric characters—likely enough to encode the selections of even a fairly long ballot. However, this QR code would have to be printed very large and might not be scannable if the paper or camera lens were smudged. Denso Wave, Incorporated. (n.d.) Information capacity and versions of the QR Code. [perma.cc/4EVV-RRSN]

[62] Los Angeles County Registrar-Recorder/County Clerk. (n.d.) BMD Ballot Security. [perma.cc/CL9L-3R6L]

[63] Los Angeles County Registrar-Recorder/County Clerk. (n.d.) Ballot Marking Device Code List. [perma.cc/WJ8B-62U5]

then checking to see if the tabulated totals match. Logic and accuracy testing can draw attention to various procedural issues with an election, allowing election officials to address them before machines are deployed. It cannot necessarily detect if a machine is compromised, however; a compromised machine could potentially “know” that it was being tested (e.g., if the date was before the scheduled start of voting) and evade detection.[64] This would be akin to Volkswagen’s “defeat devices,” which allowed cars to detect that they were being tested and activate emissions controls.[65]

***

Parallel testing and voter-reported errors

One way to avoid compromised machines “knowing” that they are being tested is to designate a subset of machines for “parallel testing,” i.e., testing while voting is occurring.[66] However, it has been argued that the amount of testing required to detect outcome-changing errors would be impractical.[67]

Another way is to depend on voter reports. In an election with compromised BMDs modifying votes in a way visible to voters who actively verify and observe those modifications, it is likely that election officials would receive an elevated number of reported errors. In order to notice a widespread issue, election officials must be monitoring election errors in real-time across a county or state.

If serious problems are revealed with the BMDs that cast doubt on whether votes were recorded properly, either via parallel testing or from voter reports, election officials must respond. Accordingly, election officials should have a contingency plan in the event that BMDs appear to be having widespread issues.[68] Such a plan would include, for instance, having the ability to substitute paper ballots for BMDs, decommissioning suspicious BMDs, and investigating whether other machines are also misbehaving. Stark (2019) has warned, however, that because it is likely not possible to know how many or which ballots were affected, the only remedy to this situation may be to hold a new election.[69]

[64] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

[65] Gates, G., Ewing, J., Russell, K., & Watkins, D. (2017, March 16). How Volkswagen’s ‘Defeat Devices’ Worked. [perma.cc/8MV2-XREA]

[66] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

[67] Appel, A.W., DeMillo, R.A., & Stark, P.B. (2020). Ballot-marking devices cannot ensure the will of the voters. *Election Law Journal: Rules, Politics, and Policy*. [perma.cc/AB7D-32BK]

[68] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

[69] Stark, P.B. (2019, August 21). There is no Reliable Way to Detect Hacked Ballot-Marking

***

Post-election auditing

The most common way to count votes in the U.S. is to tabulate the machine-readable portions of ballots with optical scanners, a fast and accurate method. However, this method has two potential problems: first, optical scanners are computerized equipment that could themselves be compromised; second, as discussed above, the machine-readable portions of ballots may not be what voters intended. It may seem that, to bypass these issues, the solution would be to count each ballot by hand.[70] Full hand counts, however, are slow, expensive, and inaccurate.[71]

Instead, post-election audits should examine the human-readable portions on a sample of ballots. Traditional post-election audits involve taking votes from a fixed random percentage of precincts, counting the ballots by hand, and comparing the totals with the totals reported by electronic tabulators.[72] However, these kinds of audits may not examine a representative sample of ballots, limiting the conclusions that could be drawn. Moreover, they may sample an unnecessarily high number of ballots (in a blowout election) or too few (in a very close one).

The solution is risk-limiting audits (RLAs), which can quickly give a high degree of confidence that the election outcome is correct while minimizing cost. In a RLA, auditors select a random sample of ballots, examining the human-readable portion by hand. Before the audit, auditors choose their "risk limit," i.e., the maximum risk that an incorrect election outcome would not be corrected by the audit – ranging from a few percentage points to 10%. The number of ballots that must be reviewed is a function of both the risk limit and the margin of the contest that is being reviewed. In a blowout election, the number of ballots to be reviewed may be very small.[73] In a close election, the number of ballots to be reviewed will be higher, but likely still far fewer than the 100% of ballots that would be counted in a full hand recount.[74]

Devices, p. 11. [perma.cc/D8YJ-MKSJ]

[70] Helderman, R.S., Gardner, A., & Brown, E. (2022, April 4). How Trump allies are pushing to hand-count ballots around the U.S. *Washington Post*. [perma.cc/9GHD-K45F]

[71] Goggin, S.N., Byrne, M.D., & Gilbert, J.E. (2012). Post-Election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence. *Election Law Journal*. [perma.cc/CQS6-PG2M]

[72] National Conference of State Legislatures. (2022, April 1). Post-Election Audits. [perma.cc/3FR7-EEVF]

[73] In such cases, it is possible that voters may not feel reassured by an RLA when informed of the small sample size. Dalela, A., Kulyk, O., & Schürmann, C. (2021, September 15). Voter Perceptions of Trust in Risk-Limiting Audits. *arXiv*. [perma.cc/5DLC-AMGJ]

[74] Lindeman, M. & Stark, P. B. (2012, March 16). A gentle introduction to risk-limiting audits. *IEEE*

RLAs are increasingly being deployed nationwide. Several states – Rhode Island, Colorado, and Virginia – have already adopted some form of RLAs. Other states have implemented RLA pilot programs in statute.[75] However, the majority of states have not yet implemented RLAs.[76]

***

Are RLAs sufficient to protect against BMD attacks?

RLAs offer the best way to detect and correct potential errors or attacks on electronic voting. RLAs should detect any attacks that occur downstream from voter verification, including the "inconsistent barcode attack" and any attacks on scanners and tabulators.

But they cannot protect against everything – for instance, a denial-of-service attack that causes voters to turn around and go home causes irreversible disenfranchisement that an RLA cannot address.

Nor can RLAs detect errors that corrupt the evidence trail of voters' choices. For instance, if a compromised BMD alters the human-readable portion of the ballot on a large number of ballots without detection, the outcome of the election could be incorrect, and an audit would accomplish little. This makes it critical to ensure that as many voters as possible examine and verify their ballots. Another way that the evidence trail could be corrupted (unrelated to BMD failures) is if proper chain of custody of ballots is not maintained; this could potentially result in ballots being added to or subtracted from the record.[77] Providing strong evidence that an election outcome was correct therefore requires a meaningful, voter-verified evidence trail – the foundation of a good post-election audit.[78]

Security and Privacy. [perma.cc/6VMM-793W]
Verified Voting. (n.d.) What is a Risk-Limiting Audit? [perma.cc/65DZ-R5GN]

[75] National Conference of State Legislatures. (2021, September 16). Risk-Limiting Audits. [perma.cc/62NM-SEWZ]

[76] Verified Voting. (n.d.) Audit Law Database. [perma.cc/9UP7-H4MV]

[77] Verified Voting. (n.d.) What is a Risk-Limiting Audit? [perma.cc/65DZ-R5GN]

[78] Stark, P.B. & Wagner, D.A. (2012, May 8). Evidence-Based Elections. *IEEE Security and Privacy*. [perma.cc/YE8T-4XR7]

Recommendations

Computerized voting systems are a key component of U.S. elections infrastructure. As with all software-based systems, it is not possible to entirely eliminate the possibility of errors, malfunctions, or attack. However, there are many things we can do to maintain and improve the security and trustworthiness of our elections. These recommendations should also have the secondary effect of deterring an attacker who wants to be undetected.

***

Conduct post-election risk-limiting audits

As described above, RLAs are one of the most effective, efficient, and inexpensive ways to catch and correct errors in election results.[79] Accordingly, over a dozen states perform some form of RLA.[80] But election jurisdictions cannot simply implement RLAs overnight. Because RLAs depend on sampling ballots at random across a state or district, the manner in which ballots are stored, organized, and numbered is important. Election officials may have to do several pilot tests in order to establish procedures that work best for them. The two-part "Knowing It's Right" series by Jennifer Morrell should help state and local election officials begin implementing RLAs.[81] A recent paper by Matt Bernhard of VotingWorks details some of the assumptions implicit in the RLA process, as well as security threats to the audit and ways to defend against them.[82]

***

[79] Lindeman, M. & Stark, P. B. (2012, March 16). A gentle introduction to risk-limiting audits. *IEEE Security and Privacy*. [perma.cc/6VMM-793W]

[80] National Conference of State Legislatures. (2021, September 16). Risk-Limiting Audits. [perma.cc/62NM-SEWZ]

[81] Morrell, J. (2019, May). Knowing It's Right, Part One: A Practical Guide to Risk-Limiting Audits. *Democracy Fund*. [perma.cc/WSC8-NNUH]
Morrell, J. (2019, May). Knowing It's Right, Part Two: Risk-Limiting Audit Implementation Workbook. *Democracy Fund*. [perma.cc/6ZNK-7JPD]

[82] Bernhard, M. (2021, October). Risk-limiting Audits: A Practical Systematization of Knowledge. *Proceedings of the Seventh International Joint Conference on Electronic Voting*. [perma.cc/EKV8-QQ98]

Encourage voters to verify their ballots

Many attacks on BMDs can only be detected by voters themselves – a form of security called "human in the loop."[83] Therefore, to strengthen security against these attacks, elections must be designed in a way that encourages voters to verify their ballots.

As described above, the evidence on whether voters can and do verify their ballots is mixed. It seems that, absent intervention, few voters do. But there is also evidence demonstrating that procedural interventions can substantially improve verification rates.[84]

In general, polling places should be designed such that voters understand that verification is a part of the voting process. Voters are probably more likely to verify their ballot if, for example, they are directed to a "ballot verification station" after receiving their paper ballot, and given verbal or written instruction. It may also be helpful for election officials to use public service announcements and other communications to inform voters ahead of time that they are a key component of election security and that they should check their ballots to ensure a secure election.[85]

***

Conduct research on methods for increasing voter verification

Given the widespread deployment of BMDs in the U.S.[86] and the importance of voter verification, it is key that we have a firm understanding of how voters behave and what interventions are most effective. But overall, there have been just a handful of studies into voter verification, covering only a handful of states. This is an area where more research – both observational studies in real polling places, and experimental studies in controlled, simulated polling places – is needed in order to determine the most effective ways to boost real-world verification rates.

[83] Cranor, L.F. (2008, April). A Framework for Reasoning About the Human in the Loop. *USENIX*. [perma.cc/PFJ4-HCPP]

[84] Kortum, P., Byrne, M.D., Azubike, C.O., & Roty, L.E. (2022, April 20). Can Voters Detect Errors on Their Printed Ballots? Absolutely. *arXiv*. [perma.cc/RP43-9V77]
Niesse, M. (2021, July 27). Under half of Georgia voters checked their paper ballots, study shows. *Atlanta Journal-Constitution*. [perma.cc/E6HD-SMVE]

[85] Kortum, P., Byrne, M.D., Azubike, C.O., & Roty, L.E. (2022, April 20). Can Voters Detect Errors on Their Printed Ballots? Absolutely. *arXiv*. [perma.cc/RP43-9V77]
Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K., & Halderman, J.A. (2020). Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *2020 IEEE Symposium on Security and Privacy*. [perma.cc/KDD8-F375]

[86] Verified Voting. (n.d.). The Verifier — Election Day Equipment — November 2022. [perma.cc/FU9P-WKAW]

Whitney Quesenbery at the Center for Civic Design has written that raising verification rates requires a holistic approach to the voter experience.[87] The BMD interface and printed ballot, the instructions given to voters, and the overall process must all be designed with voter verification in mind. Further research on effective, verification-promoting design is also warranted.

***

Have a plan for machine malfunction

Ensuring voter verification is essential – but if BMDs appear to be malfunctioning, how will election officials find out? What should they do? Widespread errors may be difficult for officials to identify quickly if there is not a process for tracking and communicating errors to a central authority.

To increase the likelihood of quickly identifying errors, poll workers and election administrators should implement processes for tracking the rate of spoiled ballots and machine errors during elections. Election administrators should set a threshold for the quantity of errors that is suspicious and which will trigger a contingency plan when exceeded. These contingency plans could include, for example, the ability to decommission voting equipment and continue the election on paper ballots if necessary – an intervention that would in turn require polling places to have the ability to print paper ballots on demand.[88]

***

Track failures in voting systems

State and federal administrators and legislatures should be empowered to track problematic machines over time across the nation to identify recurrent problems with election equipment. A 2010 report from the Brennan Center suggested that the U.S. Election Assistance Commission (EAC) create a central database of machine errors so that vulnerabilities, bugs, and coordinated attacks could be identified and addressed.[89] The need for such a database remains, though the EAC does currently provide a public list of "System Advisory Notices" indicating problems with EAC-certified voting systems.[90]

[87] Quesenbery, W. (2019, November 14). Ensuring that voters verify their ballot needs a holistic approach. *Center for Civic Design*. [perma.cc/BW7C-Q7LM]

[88] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]
Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K., & Halderman, J.A. (2020). Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *2020 IEEE Symposium on Security and Privacy*. [perma.cc/KDD8-F375]

[89] Norden, L. (2010, September 13). Voting System Failures: A Database Solution. *Brennan Center for Justice*. [perma.cc/H8WE-U924]

[90] U.S. Election Assistance Commission. (n.d.). Quality Monitoring Program. [perma.cc/4CWT-

***

Research optical character recognition for tabulation of BMD-printed ballots

As long as BMDs encode voters' choices in both a voter-verifiable form (i.e., printed text) and in a machine-readable form (i.e., in a barcode or in the position of filled bubbles), there is a potential risk that the machine-readable form could be altered, affecting the electronic tabulation. This risk is potentially limited if sufficient numbers of voters verify their ballots and if RLAs are performed regularly and consistently – as we recommend.

However, the risk can be eliminated if the only record of the vote is the printed text and if tabulators interpret the record in the same way as voters.[91] In such a system, optical scanners would have to read and interpret the printed text using optical character recognition (OCR) technology. To our knowledge there is only one commercially-available voting system in use in the U.S. that uses OCR to scan ballots.[92] Other vendors should consider offering systems that only print and scan voter choices in human- and machine-readable text.

Some have suggested that OCR cannot match the speed and accuracy of barcode scanning,[93] but OCR should be readily achievable in the polling place and at counting sites with modern hardware and software. The U.S. Postal Service, for instance, has since 1965 used OCR to sort mail.[94] Reading printed ballots (along with filled bubble location), while not trivial, should be an easier task than reading handwritten addresses; with the exception of write-in candidates, the text is computer-printed and the possible text strings can be known in advance by the scanner.[95]

QCHD]

[91] Wallach, D.S. (2019, December 12). On the security of ballot marking devices. *arXiv*. [perma.cc/2NQ8-UNDE]

[92] The Hart InterCivic Verity Duo system, which appears to be deployed primarily in Kentucky and Texas, uses OCR to scan ballots. Printed ballots still have a QR code on them for verification purposes. Hart InterCivic, Inc. (2019, October 29). Hart InterCivic's Newest Patent Protects Ballot Integrity. [perma.cc/5GU3-TC3L]
Verified Voting. (n.d.). The Verifier — Search — November 2022. [perma.cc/ZBM6-Z4D6]
Canter, J.M., Tinney, D.E., & Konovalenko, I. (2021, May 11). OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS (U.S. Patent No. 11,004,292). U.S. Patent and Trademark Office. [perma.cc/B5Q8-TFNE]

[93] VotingWorks. (n.d.). Barcodes Are a Distraction: Focus on Audits. [perma.cc/AT5B-APU2]
Quesenbery, W. (2018, May 13). Why not just use pens to mark a ballot? *Center for Civic Design*. [perma.cc/H4HW-GJLA]

[94] U.S. Postal Service. (2020). The United States Postal Service: An American History, p. 67. [perma.cc/9KUZ-NJKC]

[95] Researcher Juan E. Gilbert's Prime III research team has implemented such a system,

Despite the promise of OCR-based scanning, relatively little research is publicly available on efforts to adapt OCR to the voting domain. We think that this is a promising area for further research and product development. In addition to eliminating attacks on ballot barcodes, it may boost voter trust to remove non-voter-verifiable information from the ballot.

***

Speed the move towards VVSG 2.0-certified systems

The federal U.S. Election Assistance Commission (EAC) is responsible for drafting and adopting the Voluntary Voting Systems Guidelines (VVSG), a set of standards for voting systems that states may voluntarily adopt. A majority of states require some aspect of the EAC's standards, with 11 states and the District of Columbia requiring that their systems be fully certified to the VVSG.[96] In February 2021, the EAC adopted the first major update to the Voluntary Voting Systems Guidelines in 15 years: VVSG 2.0. The new requirements included in VVSG 2.0 would go a long way towards addressing the possible attacks described above.

VVSG 2.0 requires new security protections that could make hacking a BMD more difficult. For instance, it requires multi-factor authentication to verify the identity of a user performing critical operations, such as tabulating results. It also establishes a framework by which users are only allowed to perform the functions necessary for their specific role in the election.[97] Additionally, it limits the exposure of physical (e.g., USB) ports when unnecessary.[98]

The guidelines would also enhance barcode transparency, requiring that manufacturers and systems document how selections are encoded in barcodes, such that a voter can "understand the barcoded contents."[99]

called Informed OCR, into their voting machine. Clemson University RAAV Final Report, p. 7. [perma.cc/L96K-22XX]

[96] National Conference of State Legislatures. (2021, November 5). Voting System Standards, Testing and Certification. [perma.cc/XCW6-8QDD]

[97] U.S. Election Assistance Commission. (2021, February 10). Requirements for the Voluntary Voting System Guidelines 2.0, Requirement 11.3. [perma.cc/69QT-TYHC]

[98] U.S. Election Assistance Commission. (2021, February 10). Requirements for the Voluntary Voting System Guidelines 2.0, Requirement 12.2. [perma.cc/T4P9-MM52]

[99] U.S. Election Assistance Commission. (2021, February 10). Requirements for the Voluntary Voting System Guidelines 2.0, Requirement 3.3. [perma.cc/8ER2-9SA3]

Critically, the guidelines include an entire section ensuring that voting systems are auditable.[100] As described above, VVSG 2.0 includes the requirement that systems be fully software independent, ensuring that voting systems and elections can be audited without having to trust that the software is functioning properly. It includes other requirements that will ease the implementation of the post-election audits we recommend here, such as the requirement that a voting system be able to print unique identifiers on cast ballots for auditing purposes.

There are currently no voting systems available that are certified to VVSG 2.0. Before those systems can be made available to election officials, the Voting System Test Labs must be prepared to test voting systems against the guidelines.[101] At this point, however, the labs are not ready. Once they are, vendors can begin submitting their systems for testing and certification.

In the meantime, election vendors should be working to make sure that new systems incorporate as many VVSG 2.0 requirements as possible, in advance of lab testing. The major election vendors in the U.S. claim to be doing so, but it would be beneficial to have more transparency and communication about what features they are adding or changing to new systems.[102] These vendors have estimated that VVSG 2.0 systems will not be submitted for testing until after the 2024 general election. Another vendor, VotingWorks, also says they are working to comply with VVSG 2.0.[103] VotingWorks makes all of their voting system code openly available so that anyone can track their progress online.[104]

State and local election officials should also let technology vendors know that they are interested in operating VVSG 2.0-certified systems as soon as they are available – making clear that there is a demand for systems with modern security protections and auditability. And state legislators who are interested in election integrity should make clear that funding will be made available to purchase these systems once they are available.

[100] U.S. Election Assistance Commission. (2021, February 10). Requirements for the Voluntary Voting System Guidelines 2.0, Principle 9. [perma.cc/8W69-HNBD]

[101] U.S. Election Assistance Commission. (n.d.). VOLUNTARY VOTING SYSTEM GUIDELINES. [perma.cc/WT47-DQWH]

[102] Dominion Voting Systems, Election Systems & Software, Hart InterCivic, MicroVote, Smartmatic, & Unisyn Voting Solutions. (n.d.) Frequently Asked Questions about the VVSG 2.0. [perma.cc/FSJ7-NGRY]

[103] Childers, M.C.C. (2021, December 20). The Road to VVSG 2.0 Certification. *VotingWorks*. [perma.cc/ZJH9-RAEN]

[104] VotingWorks. (2022). Vx Complete System [Source code]. *GitHub*. [perma.cc/FU6U-26CF]

Conclusion

Although the 2016 Russian attacks were primarily targeted at other components of U.S. election infrastructure than those discussed here, they highlighted the threat and possibility of foreign interference and hacking. But the aftermath of the 2020 election might indicate an even greater threat: the infiltration of domestic actors who seek to undermine free and fair elections.

Rampant disinformation about the integrity of the 2020 election has led many to believe false narratives about how elections are run. Proponents of these narratives appear to be gaining influence in election administration, either as poll workers[105] or as top state election officials.[106] The infiltration of "election deniers" – those who insist without evidence that the 2020 election was rigged[107] – into positions of power in administering elections poses a grave danger to American democracy: the possibility that an insider will manipulate election systems in order to bring about a desired election outcome. This elevated insider threat makes it more important than ever that our voting systems are resilient to attack and manipulation.[108] Paradoxically, though, 2020 conspiracy theories have made it more difficult to discuss election security and make necessary improvements.[109]

Electronic voting systems, including BMDs, are among the most controversial components of U.S. election infrastructure. Because of the problems outlined above, some experts recommend that BMD usage be minimized

[105] Przybyla, H. (2022, June 1). 'It's going to be an army': Tapes reveal GOP plan to contest elections. *Politico*. [perma.cc/NR5Y-ZTWB]

[106] Gardner, A. & Arnsdorf, I. (2022, June 14). More than 100 GOP primary winners back Trump's false fraud claims. *Washington Post*. [perma.cc/QRA3-V3VN]

[107] Schouten, F. (2022, June 15). Election deniers are winning political nominations across the country. *CNN*. [perma.cc/5BYZ-MABQ]

[108] Norden, L. & Tisler, D. (2021, December 8). Addressing Insider Threats in Elections. *Brennan Center for Justice*. [perma.cc/92QP-KEU4]

[109] Marks, J. (2022, June 17). Trump's false election claims made it tougher to talk about election security. *Washington Post*. [perma.cc/72CT-HCNW]

only to voters who need them for accessibility reasons – an approach which may have unintended negative consequences. On the other hand, some states have all in-person voters vote on BMDs – which could be a vulnerable and expensive way to run an election.

Despite their drawbacks, BMDs are likely to be a key part of elections for the foreseeable future. Whether BMDs are used in a jurisdiction by a small number of voters or by every in-person voter, it is important to have a reasoned conversation about their benefits and risks, and how to mitigate those risks in the short and long term.

We hope that the recommendations outlined above will enable vendors and jurisdictions to make improvements to BMDs and how they are implemented in the polling place. We should work to ensure that elections use electronic equipment in a way that maximizes security, voter verification, and auditability. With U.S. election administration potentially facing serious threats from within, there is little time to waste.

cdt.org

cdt.org/contact

Center for Democracy &
Technology
1401 K Street NW, Suite 200

202-637-9800

@CenDemTech

CENTER FOR
DEMOCRACY
& TECHNOLOGY