The Past, Present, and Future of American Election Security: A Survey

by
Lyell Read

A THESIS

submitted to

Oregon State University

Honors College

in partial fulfillment of
the requirements for the
degree of

Honors Baccalaureate of Science in Computer Science
(Honors Scholar)

Presented May 27, 2022
Commencement June 2022

AN ABSTRACT OF THE THESIS OF

Lyell Read for the degree of Honors Baccalaureate of Science in Computer Science presented on May 27, 2022. Title: The Past, Present, and Future of American Election Security: A Survey

Abstract approved:

Yeongjin Jang

The widespread adoption of computerized systems around the turn of the century as a means of more efficiently conducting elections introduced more issues than these computer systems were intended to address. Though many of these flaws were not considered for years or decades after the introduction of digital election infrastructure, it has recently become apparent that a minimal emphasis was placed on securing these systems. As a result, the election hardware on which America conducts its elections today is largely insecure and antiquated. This has sparked a series of recommendations for modern technological systems to take the place of older, insecure machines. Often, however, the novel approaches to election security neglect some of the most important attributes of a trustworthy election such as an authoritative paper trail and the requirement of voter privacy. As a result, many proposed solutions offer no more security or trustworthiness than the status quo. In this paper, we present the background for – and security of – the current state of US election technology. We use this background to consider propositions for futuristic election schemes, and examine these against the characteristics of a secure, trustworthy election.

Key Words: US Elections, Election Security, End to End Verifiability, Blockchain Voting

Corresponding e-mail address: readly@oregonstate.edu

The Past, Present, and Future of American Election Security: A Survey

by
Lyell Read

A THESIS

submitted to

Oregon State University

Honors College

in partial fulfillment of
the requirements for the
degree of

Honors Baccalaureate of Science in Computer Science
(Honors Scholar)

Presented May 27, 2022
Commencement June 2022

Honors Baccalaureate of Science in Computer Science project of Lyell Read presented on May 27, 2022.

APPROVED:

Yeongjin Jang, Mentor, representing Computer Science

Vincent Immler, Committee Member, representing Computer Science

---

Dave Nevin, Committee Member, representing Computer Science

Toni Doolen, Dean, Oregon State University Honors College

I understand that my project will become part of the permanent collection of Oregon State University Honors College. My signature below authorizes release of my project to any reader upon request.

Lyell Read, Author

The Past, Present, and Future of American Election Security: A Survey

Lyell C. Read
readly@oregonstate.edu
Oregon State University

Abstract

The widespread adoption of computerized systems around the turn of the century as a means of more efficiently conducting elections introduced more issues than these computer systems were intended to address. Though many of these flaws were not considered for years or decades after the introduction of digital election infrastructure, it has recently become apparent that a minimal emphasis was placed on securing these systems. As a result, the election hardware on which America conducts its elections today is largely insecure and antiquated. This has sparked a series of recommendations for modern technological systems to take the place of older, insecure machines. Often, however, the novel approaches to election security neglect some of the most important attributes of a trustworthy election such as an authoritative paper trail and the requirement of voter privacy. As a result, many proposed solutions offer no more security or trustworthiness than the status quo. In this paper, we present the background for – and security of – the current state of US election technology. We use this background to consider propositions for futuristic election schemes, and examine these against the characteristics of a secure, trustworthy election.

1 Introduction

US Congress introduced Help America Vote Act (HAVA) in 2002 to address the apparent failings of the presidential election of 2000. Hanging chads, undervoting and recounts were widely publicized as a result of the closeness of the race which served to establish negative opinions about punch card voting. HAVA is significant as it was the impetus for a transition to electronic voting machines – machines supposed to fix the flaws of the punch cards blamed for the failures in 2000 [1].

The solutions chosen to supplant punch ballot voting are notable for almost unanimously featuring computerization to achieve their functionality. In some cases, the essential[1] part of the old system – the paper ballots themselves – were omitted from the design of the new systems funded and mandated by HAVA. Compounding this problem, the rise in prominence of computer usage between 2000 and 2016 saw a commensurately increased interest in cybersecurity. Elections, as critical infrastructure, naturally became the unfortunate target of attacks [2]. These attacks are facilitated by several issues inherent to the bureaucracy and finances of procuring and maintaining election equipment, namely that the voting systems adversaries are targeting are long outdated and severely vulnerable. Infrequently, the public can perceive these issues in voting technology through contracted reports and at conferences such as DefCon [3–11], however the advent of such publications is a recent occurrence. To address these shortcomings, academia and the corporations have proposed numerous designs for novel election schemes.

In this paper, we review the relevant historical background about election technology before examining a collection of currently operated election equipment in detail. This includes a detailed look at a representative machine from each major class of actively used voting machines. This discussion includes publicly disclosed flaws in these machines presented in the context of the machine's threat model which is in turn based on the machine's typical usage. To contend with the future propositions for elections, we evaluate two schemes representing different approaches to applying high technology to elections. The first is a blockchain-based voting concept, the latter is a Software Development Kit (SDK) for implementing End-to-End (E2E) verifiability in elections. This paper closes with a summary reconciling the promise of high technology in elections and the current state of election security with a focus on the steps to take going forward.

This paper provides the following contributions:

- We provide a summary of the current state of election technology and security. This is combined with a threat

[1] Original HMPB are essential in that they serve as an authoritative set of votes cast which can be used in audits and recounts.

model specific to each machine class.

- We then provide a contextualization of known vulnerabilities against existing systems and gauge their impact against a set of attacker goals.
- We examine two recent proposed election schemes, a Blockchain-based scheme proposed by Ayed [12] and Microsoft ElectionGuard [13]. We compare these with the conditions required for an ideal election. In cases where these schemes are vulnerable to attacks against the core requirements of an ideal election, we provide a description of the attack.
- We close with a conclusion based on the evidence presented in this paper, summarizing the best practices for elections in the future and recommendations for proceeding with election system modernization.

1.1 Limitations

The topic of voting technology security is vast. There are innumerable technologies interacting to complete an election. As a result, this paper is limited in scope, and contains compromises in content. We outline the limitations of this work in this section.

This report is limited to the study of the voting machines and the software present on them. Election systems manufacturers also design and sell (often bundled with voting machines) software suites which permit election officials to design election specifications and simplify the aggregation of tallies [14]. These systems, while not included in this paper, have been found to be vulnerable and represent a significant threat to election security as detailed in past reports, namely the EVEREST report [6].

This paper is also limited when considering the existing data about voting machine vulnerabilities. We rely on the reports from the Voting Machine Hacking Villages at DefCon 26 [3] and 27 [4] – reports of compiled findings from members of the public who examined available voting systems for vulnerabilities – despite these reports not constituting peer-reviewed research. This is because, excluding these reports, the professional analyses of voting machine vulnerabilities are few and far between. The lacking availability of more reliable information on this topic is a direct result of election technology manufacturers consistently adopting a security-by-obscurity or black box approach to the security of their machines. This results in limited data being available about the flaws in voting machines as no reviews of these are rarely sanctioned by the manufacturers[2]. This compromise is partly addressed by the fact that the results of the DefCon Voting Machine Hacking Village reports include findings the author has personally discovered or verified.

[2]When reviews are sanctioned, they tend to be highly restrictive.

As a direct consequent of the two limitations above, it is not feasible to present an exhaustive set of vulnerabilities or attack methods endangering current US election infrastructure. In part because many such vulnerabilities have yet to be found, and as a result of the variety of technologies used in US elections, this report contains a fraction of vulnerabilities which affect elections in the US.

In addition, we omit a separate examination of mail-in voting under the assumption that the same tallying machines used for this purpose are used for centrally scanning Hand Marked Paper Ballots (HMPB) and BMD-marked ballots during an in-person election [15]. Similarly, we do not discuss the issue of Email voting for absentee voting.

Lastly, this paper does not cover certain requirements of an election as discussed in Section 2.2. These are omitted for brevity. We also exclude discussion of voter registration, polling and the associated hardware for each. While these are important parts of an election, we focus on the machines charged with casting, recording and tallying votes.

As well, we partially restricted the threat model we apply to voting systems described in this paper. These limitations are described in Section 2.3.1.

2 Background

In this section, we introduce the historical background which justifies the current widespread usage of digital election equipment. This includes a rough timeline of noteworthy developments in election technology.

In order to contextualize claims about the aptitude of an election scheme for use in a real election, we describe both what conditions must hold for an election to be trustworthy as well as the threat model for an attacker threatening election infrastructure.

2.1 Historical Context

Through the years, the US has experimented with a variety of types of voting machines, each waxing and waning in popularity as time passes. Beginning in 1889, the mechanical lever voting machine was patented, and saw use in the US beginning in 1892 in Lockport, New York [16]. From here, it is estimated that by 1930, the US used mainly lever machines. In 1962 and 1964 respectively, optical scanners and punch card tally machines were first used [17]. The first Direct Recording Electronic (DRE) machine was patented in 1974 [18] and began to see use almost immediately. By the election of 2000, punch card machines made up the majority of voting systems, with the relatively new optical scanners and DREs also seeing increased use since their conception [17, 19].

The 2000 election proved to be a significant turning point for the choice of election technology. The debacle in Florida around "hanging chads" [1] during this election was the impetus for HAVA in 2002, an act with the goal of moving America

away from the punch card voting systems blamed for the issues in the 2000 election. This act, however, called for more widespread usage of DREs despite the publication of research indicating that optical scanners should be the target of investment [20]. The author of HAVA conceded this suggestion for investment into optical scanners was correct, albeit after HAVA became law [1].

After 2000, the US saw a shift in choice of election technology. Punch card machines were practically nonexistent by 2008 and lever machines by 2012. At the time of the 2016 election, the US relied primarily on optical scanners and DREs for voting [19, 21].

Since 2016, the major change in election technology has been the adoption of BMDs. These machines are used to mark a ballot as a voter indicates whether on a screen or using push-buttons. The BMD then prints the ballot, which is aggregated for manual or optical tabulation. As of 2022, the non-profit Verified Voting estimates that 68.9%[3] of the US uses hand-marked paper ballots, 23.2%[4] BMD-marked ballots and 8%[5] DRE systems [19, 21].

2.2 Conditions of a Trustworthy Election

Whether an election involves digital or physical machines, there exists a set of characteristics that all elections must meet – a set of requirements which makes creating secure elections one of the tougher challenges of our time. The requirements can be organized into three categories: privacy, verifiability and general [22]. As discussed in Section 3, the current US election system represents a compromise of some of these requirements in order to have a functional system of any kind.

2.2.1 Privacy

This requirement is concerned with ensuring that a voter cannot be shown to have voted a given way, nor can they prove that they voted in such a way. These privacy protections in turn assure that it is impossible to coerce a voter, as the voter cannot prove how they voted. This encompasses three requirements which, eliminate any possibility of coercion. The requirements are as follows:

Ballot Secrecy ensures that the voting scheme can not reveal how an individual voted using that system [22–25].

Receipt-Freeness asserts that the receipt provided to a voter after they cast their ballot does not contain any indication of how the voter voted [22, 24, 25].

Coercion-Resistance dictates that the voting scheme must not permit the voter to be coerced to vote a certani way [22–25].

In practice, the privacy requirement of elections tends to be the most difficult of the requirements examined in this section. In most implementations, Ballot Secrecy makes many of the verifiability requirements described below difficult or impossible [22, 24, 26].

2.2.2 Verifiability

Verifiability is often invisible as it exists in our current US election scheme. Currently performed mainly through auditing (and even then, not entirely attaining the requirement of verifiability) [24], this set of requirements are those of a perfect election. Unattainable as they might be in the current system which prioritizes other requirements of Ballot Secrecy and the general requirements below, the following classes of verifiability are essential components in a perfect election scheme:

Cast-as-Intended asserts that the vote indicated by the user is correctly registered on the output of the system casting the ballot [22–25].

Recorded-as-Cast makes sure that the voter's cast vote is accurately recorded in the voting system [22–25].

Tallied-as-Recorded ensures that the recorded vote is counted in the final tallies for the election [22–25].

As indicated above, the requirements that make up verifiability are often at odds with those of privacy. Some technologies suggested later in Section 4 discuss the technical approaches to this issue.

2.2.3 General

Any election scheme has a multitude of baseline requirements which ensure that it functions, and does so in accordance with the law. The general requirements of an election are: eligibility verification [25], accountability for failures, robustness, usability, and accessibility [22]. Each of these requirements exist regardless of the scheme to ensure an election will function properly. As mentioned in Section 1.1, these general requirements are treated as implicitly required of all elections throughout this paper.

2.3 Modern Election Threat Model

In this section, we discuss the ways election schemes can come under threat, and what the goal of an attack would be. To do this, it is necessary to define a threat model in order

[3] Percentage of registered voters living in jurisdictions using HMPBs for most voters [21].

[4] Percentage of registered voters living in jurisdictions using BMDs for all voters [21].

[5] Percentage of registered voters living in jurisdictions using DREs for all voters [21].

to be precise about the avenues of attack against election infrastructure. In this section, we define a *threat* to be the danger an attacker wishing to accomplish an attack poses to the target system.

2.3.1 Threat Model Limitations

We restrict the threat model to only concern attacks that involve a maliciously-inclined voter, poll worker or election official altering a physical voting machine through direct interaction with that system.

Notably excluded from the threat model are the socio-political conditions in which election schemes exist. While this topic is certainly worth considering in depth when analyzing elections as a whole, the scope of this issue is beyond that of this paper.

There exist threat models for all parts of the election process, including those which are not covered in this paper, such as voter registration and the use of pollbooks in election schemes. These are omitted to focus on the threats posed to casting, recording, and tallying of votes themselves.

2.3.2 Successful Attack Outcomes

In this section, we define the attacker's capabilities and goals when attacking an election scheme. As is done by the Cybersecurity and Infrastructure Security Agency (CISA) [27], we associate most attacker goals with a violation of one or more of the Confidentiality, Integrity, Availability (CIA) triad. We selected these goals as the most impactful goals an attacker can have against an election scheme. This is not an exhaustive list of the goals an attacker may have.

We assume that any attacker targeting an election system has the ability to acquire and reverse engineer the firmware or source code of the target machine. Further, we assume that this attacker has the adequate tools and knowledge to design exploits that make use of vulnerabilities in the machine to accomplish their goals. This attacker also has physical access to the machine, whether as a voter, poll worker or election official.

1. **Attack 1: Modifying Election Results** is usually the most desirable goal for an adversary attacking an election scheme or machine. This attack would be successful if an attacker can alter the final tally of votes which a device outputs to be different from the actual composition of votes or ballots processed. At the largest (national) scale, this attack would have as its goal to alter the result of an entire election. Modifying election tallies violates the integrity of the targeted system or election [6, 27].

2. **Attack 2: Reducing Voter Trust in Election Scheme** is concerned with undermining public confidence in the current election scheme. This often is accomplished by disseminating information aimed at diminishing public trust in the existing election infrastructure. If an attack succeeds in reducing voter confidence in their election infrastructure, this attack might have violated any part of the CIA triad [6].

3. **Attack 3: Preventing Election from Running**, commonly referred to as a Denial of Service (DoS) attack, is an attack which renders part or all of an election inoperable. This involves incapacitating any number of services or devices an election relies on. The successful completion of a DoS attack against an election affects the availability of the targeted election [6, 27].

4. **Attack 4: Disclosing Voter Choices** entails violating the requirement of Ballot Secrecy by disclosing the way individual voters cast their votes. The violation of Ballot Secrecy in this manner has the immediate result of invalidating Coercion-Resistance and is likely to have the tertiary effect of drastically reducing voter trust in this election scheme. This attack, if successful, would violate the confidentiality of the election scheme [6, 27].

3 Present State and Vulnerabilities

In this section, we discuss the current state of election systems and the security thereof. As discussed in Section 1.1, this report does not contain an exhaustive set of machines or vulnerabilities. Instead, this section attempts to establish the most common machines in use in the US and how these machines are used in an election. Moreover, we examine known vulnerabilities in similar machines which have been publicly disclosed. Based on this, we synthesize what an adequately motivated, funded, and determined attacker can likely do in the context of the attacks outlined in Section 2.3.2.

3.1 US Elections and Their Machines

The US has an innately varied set of election systems as a result of the choice of voting equipment and modality being largely delegated to individual states. This has the inevitable consequence that each state has different machines in different numbers than the next state. This in turn makes it difficult to exhaustively list the devices and vulnerabilities of the current system. Despite variation, there exist a handful of devices with wider adoption than others. These machines represent a significant portion of the population. Unfortunately, this set of widely used device is mostly disjoint from the set of devices which have been analyzed from a cybersecurity standpoint.

Election modality also varies by state. As of 2022, there are 8 states conducting all elections by mail, the remaining states require (in most cases, usually excluding absentee voting) in-person voting for most large elections and varying modalities for smaller elections [28]. Despite this difference, the machines used for tallying mail-in votes are similar to

those used in different states for ballot scanning. To scan and tally ballots, Batch-Fed Optical Scanners (BFOS) or Hand-Fed Optical Scanners (HFOS) are present in almost all election schemes for tallying HMPB or Ballot Marking Device (BMD) marked paper ballots even if those HMPB are mail-in ballots [21]. Therefore, while the modality informs aspects of the threat model not covered in this paper, it often does not alter the machines used or their vulnerabilities.

We chose three classes of machines for this report, as they represent the most prevalent devices currently in use in the US. These classes are:

Optical Scanners are responsible for a majority of the scanning and tabulation of ballots across the US[6]. These machines fall into one of two categories: manually operated HFOS, usually operated by voters, and BFOS which are usually present in a central location for rapid tabulation of large quantities of ballots [21].

Ballot Marking Devices (BMDs) are computerized systems which take a user's chosen vote as input and print out a ballot to match those choices. These machines are included in this report as 23.2% of all registered voters live in a jurisdiction that uses BMDs for all voters [21]. As well, BMDs are one of the two major ways in which voters mark their ballots nationally[7].

Direct Recording Electronic (DRE) represent 8% of registered voters who live in jurisdictions requiring the use of DREs for all voters [21]. DREs simplify the process of casting a vote – a voter's only task is to use the touchscreen to select their choices, and sometimes verify these choices before their ballot is cast.

Once we defined these three classes of voting machines, we compiled data from the Verified Voting project and processed it as described in Appendix B in order to generate rough estimates for the make and model of the machines available to the most voters in the US. This yielded the top 3 machines in each category by *population share*[8] as of 2022 [21] shown in Table 1.

We derived another set of machines from the Verified Voting dataset. This set of machines includes one machine from each of the categories above (explicitly differentiating HFOS and BFOS as their threat models differ). This machine from each category was selected to be a machine which has been analyzed by researchers or participants in an open hacking event, such as the DefCon Voting Machine Hacking Village. This set of machines is displayed in Table 2.

Type	Make	Model	Pop. Share
HFOS	ES&S[9]	DS200	∼24.5%
BFOS	DVS[10]	ImageCast Central	∼15.0%
BFOS	ES&S	DS850	∼14.7%
	–	Other	∼45.8%
BMD	ES&S	ExpressVote	∼37.0%
	DVS	ImageCast X BMD	∼21.3%
	ES&S	AutoMARK	∼11.6%
	–	Other	∼30.1%
DRE	DVS	ImageCast X DRE	∼29.6%
	SVS[11]	AVC Advantage	∼23.0%
	Microvote	Infinity	∼15.1%
	–	Other	∼32.2%

Table 1: Top three machines with the largest population share in their machine class. The optical scanner category includes both BFOS and HFOS.

In the following sections, we present vulnerabilities found in these machines and the implications with regards to the threat model and attacks outlined in Section 2.3.2. Then, we discuss how these vulnerabilities could affect an election were they present in machines with a higher population share such as those presented in Table 1.

3.2 Hand Fed Optical Scanners

An election employs HFOS to process marked ballots and tabulate the results. HFOS accept ballots entered manually into the machine for counting. Given the reduction in processing capacity incurred by manually entering ballots into HFOS, these are often used by the voter in the same location where they mark their ballot. HFOS can be referred to as "precinct scanners" [19] or "poll place ballot scanner" [29] for this reason. It is of note that in some precincts, voters are required to use these machines, and therefore come into contact with HFOSs [6, 15, 19, 30].

3.2.1 Threat Model

As HFOSs are responsible for tabulating a relatively large number of ballots[13], these machines are a desirable target for an adversary seeking to disrupt or alter an election. In order to analyze the threat model of a HFOS, one must consider three different attackers [6, 19, 30]:

- A voter, determined to modify the functioning or tallying of the machine. This voter is usually supervised in their interaction with the HFOS, therefore their options for physical attacks are limited. Despite this, a talented

[6] The remaining minority of ballots are counted by hand [21].
[7] Apart from BMDs, the rest of the paper ballots marked during an election are HMPB.
[8] Defined and explained in Appendix B
[9] See Appendix A.
[10] See Appendix A.
[11] See Appendix A.
[13] The ES&S DS200, for example, has the capacity to process and store 2,500 ballots before requiring manual attention [29].

Type	Make	Model	Pop. Share	Attack 1			Attack 2			Attack 3			Attack 4		
				V	P	E	V	P	E	V	P	E	V	P	E
HFOS	DVS	ImageCast Precinct	∼10.4%	V	V	V	V	V	V	V	V	V	U	U	U
BFOS	ES&S	Model 650	∼0.2%[12]	S	V	V	S	V	V	S	V	V	S	V	V
BMD	ES&S	AutoMARK	∼11.6%	S	V	V	V	V	V	V	V	V	S	S	S
DRE	DESI	AccuVote TSX	∼7.3%	V	V	V	V	V	V	V	V	V	S	U	U

Table 2: Machines from each machine class (explicitly differentiating HFOS and BFOS) which have undergone some form of publicly released security audit and make up a significant population share evaluated against resistance to attacks set out in Section 2.3.2. Each attack has a dedicated column for the threat model of a Voter ("V"), Poll Worker ("P") or Election Official ("E"). A machine which is vulnerable to an attack is denoted by V, one which is safe against such attacks is denoted S and in cases where the attack is exclusively speculative, we mark U. These indications do not take into account auditing such as RLAs, which can address many of these vulnerabilities.

individual might be able to interact with any open I/O ports on the device or scan a maliciously crafted ballot in order to attempt an attack [6].

- A poll worker who has direct, legitimate contact with the machine. A poll worker is tasked with configuring the parameters of election on the HFOS, and therefore accesses the administrative panel of the machine as part of preparing and tallying an election [6].
- An election official, who has all the access of a poll worker as well as permission to interact with HFOSs even while elections are not taking place and the units are in storage [6].

3.2.2 Vulnerabilities

As part of the public security audit of election equipment at the DefCon 27 Voting Machine Hacking Village, researchers analyzed the Dominion ImageCast Precinct. The machine attendees examined was a hybrid machine, incorporating both a BMD as well as a HFOS. During this engagement, researchers were able to access USB, RJ-45 and Compact Flash (CF) I/O without destructive means. On the ImageCast Precinct researchers found an outdated version of BusyBox which was vulnerable to several Common Vulnerabilities and Exposures (CVEs) including a network DoS vulnerability. Further, exposing the USB port which is first on the machine's boot priority list was trivial, permitting researchers to boot into an operating system of their choice operating system. From there, researchers were able do extract the contents of the onboard storage and found ballots stored unencrypted. It is supposed that researchers could also have modified these ballots, though this was not attempted [4].

It is worth noting that the hybrid nature of this machine puts into question the applicability of these results to HFOS. It was not documented which component of the ImageCast Precinct system (BMD or HFOS) each of these vulnerabilities applies to. Given that marked scans of ballots were found on the CF card, this indicates that at least this component is related to the optical scanning portion of the ImageCast Precinct. In Section 3.2.3 below, a note will be made at the end of each attack indicating whether this attack affects the BMD, HFOS or both.

3.2.3 Implications

Taken together, the varied routes of attack against the Dominion ImageCast Precinct system and the ease of all these attacks suggest that it would be trivial for a prepared, unobserved voter to interact with the I/O functionality of this machine, which would permit them to perform the following attacks:

1. With specially crafted malware on a USB device, an attacker could interact with the exposed USB port to perform DoS against the system (Attack 3). *(BMD)*
2. Extraction of the CF card by an attacker is likely to cause the machine to malfunction when scanning future ballots, providing another way to carry out DoS against this machine (Attack 3). *(BMD, HFOS)*
3. This access to the CF card could also permit the attacker to modify votes, should they come prepared with a properly formatted[14] CF card to replace the extracted card with, succeeding in Attack 1. *(HFOS)*
4. Given that images of ballots are stored on the CF card without encryption, this could permit the malicious attacker to verify that a coerced voter (who was instructed to specially mark their ballot somehow) voted as demanded, accomplishing Attack 4. *(HFOS)*
5. A poll worker or election official with legitimate physical access to the machine could perform attacks 1, 2, 3 and 4 listed above with ease, given preparation. *(BMD, HFOS)*
6. A poll worker or election official could install a malicious program onto this machine which tampers with

[14] This card might have to be signed as well as formatted properly in order to work in the ImageCast Precinct HFOS. The attack described remains untested and an area for future research.

cast ballots as they are stored and tallied on disk, accomplishing Attack 1. *(HFOS)*

7. Attacks 1, 2, 3, 4, 5, and 6 listed above could, if publicized, undermine public confidence in BMDs and HFOS – devices common enough to cast doubt onto the security of election schemes using HFOS. This would achieve Attack 2. *(BMD, HFOS)*

Given this variety of vulnerabilities and corresponding attacks, there is no reason to believe that similar attacks are not present on other Dominion ImageCast machines[15] such as the ImageCast Central included in Table 1. Moreover, the functioning of HFOS devices is largely the same across makes and models. Based on these, we conclude it is likely that most other HFOS devices could be compromised in a similar fashion [5, 6].

In the context of a broader election, these attacks pose minimal risk, provided that the best practices are in place. In this case, these best practices require Risk Limiting Audits (RLAs) after each election and the paper trail of ballots be present within the HFOS[16] to remain secure. With these best practices, an attack aimed at altering the outcome of an election would likely not succeed as it would be caught during the RLA, triggering a recount which would generate an accurate final tally.

Were an attack against a HFOS to succeed and go undetected by an audit, the effect on the election as a whole would depend on the number of votes an attacker had managed to alter or remove in comparison to the total number of votes cast. In a small election, this could matter greatly. In the context of a presidential election, managing to exploit a single HFOS is unlikely to alter the outcome of the election as a whole.

As far as a DoS attack against an HFOS, this action alone could both halt elections relying on these machines as well as serve to reduce voter confidence in the stability of their election infrastructure. Executing a DoS attack against a HFOS or multiple HFOS could serve to delay the election, possibly requiring the election to be re-run at a later date.

3.3 Batch Fed Optical Scanners

BFOSs are the backbone of most election systems as they are used to efficiently tally marked paper ballots. BFOSs take in a collection of ballots, usually drawn from a tray, and scan and tally them automatically according to an election definition programmed into them before the election. These machines are usually centrally located leading them to also be called "central scanners" [31] and "central ballot tabulators" [31]. When deployed, these machines are commonly centrally located, in an access controlled location. Voters do not come into contact with these machines [6, 15, 19, 31, 32].

3.3.1 Threat Model

Considering that BFOSs scan and tally a large number of ballots, these machines are a high impact target for an adversary seeking to attack an election. Performing DoS would significantly delay an election, while modifying tallies undetected could have a large effect on the outcome of the election. Given the fact that access to these machines during election day is guarded however, the only meaningful threats to BFOSs are posed by a poll worker or election official. Both of these individuals can have direct, legitimate contact with the machine. Poll workers configure BFOS for elections, and therefore have the ability to program these machines with election configurations. Election officials have these privileges as well as access these machines while they are in storage [6].

3.3.2 Vulnerabilities

Included in the machines present at the DefCon 26 and DefCon 27 conference's Voting Machine Hacking Village, the ES&S Model 650 Central Ballot Scanner system was the subject of hacking attempts by attendees. In addition, this system was professionally audited[17] by a team contracted by the Ohio Secretary of State, an effort that resulted in the EVEREST Report [6].

Through these examinations, it has become clear that this system is insecure to an attacker with physical access to the machine. The system executes the contents of a Zip Disk if present on bootup[18], does not validate election definitions, and does not protect against buffer overflows and integer overflows. Moreover, the Model 650 will accept and tally counterfeit ballots and an attacker with physical access can gain entry to the Model 650's internal storage, exposed RJ-45 port[19] and the internals of the machine by removing a ventilation fan or picking the simple access door lock [3, 4, 6].

3.3.3 Implications

Combined, these make the Model 650 vulnerable to Attacks 1, 2 and 3. Specifically, with the aforementioned vulnerabilities, a poll worker or election official could accomplish the following attacks:

[15] ImageCast is the name of a line of products offered by Dominion.

[16] Election security researchers have yet to find a machine which can provide adequate physical security to keep determined hackers out of any locked area [3,4]. In this section, we assume that even with access to the ballot compartment, it would take a significant amount of time to remove ballots to skew the count to match the modified count on the machine. With the time constraints of an election and voters, poll watchers and fellow election officials looking on, modifying a HFOSs paper trail is not feasible.

[17] Along with several other ES&S voting machines and the accompanying ES&S Unity software suite and other, discussion of which will not be part of this report as outlined in Section 1.1.

[18] This requires the disk be formatted and two files with specific names to be created on the disk [3].

[19] While present on the machines at DefCon, it is not clear whether this is a manufacturer upgrade or a feature present on all Model 650 BFOS.

1. An attacker can gain arbitrary code execution on the Model 650 using the fact that it executes Zip Disk on startup. Using this, this attacker can possibly DoS the system by installing a corrupted election definition or malware (Attack 3).

2. Using arbitrary code execution from the Zip Disk vulnerability described in attack 1 above, a malicious poll worker or election official could also write malware to silently alter the recording of votes. This would accomplish Attack 1.

3. Using the low physical security of the device, an attacker could trivially damage or disconnect internal components resulting in DoS (Attack 3).

4. An election worker could design a faulty ballot definition to cause the machine to either not scan votes for a particular race or candidate at all, or subject specific parts of a ballot to higher error rates during scanning. Through this, they could modify the results of an election, accomplishing Attack 1.

5. Attacks 1, 2, 3 and 4 presented above would undermine the trust of voters if revealed, accomplishing Attack 2. Often, the Model 650 and other BFOSs are used for mail-in voting, which places a large amount of trust on the election equipment and operators – trust which has seen increased scrutiny after the 2020 election [33].

Given these, we posit that other similar vulnerabilities are present on other related machines such as the Model 150 or newer ES&S machines. Even in other BFOSs, like those listed in Table 1, we believe that similar attacks are possible.

In the context of a broader election, an election official can disrupt an election or alter votes on a small scale even with the presence of RLAs using these vulnerabilities. To accomplish this, the attacker would have to be an election official with knowledge of election procedures. This person would be more familiar than a voter with how election are conducted and know how to modify the paper trail to match their modified tallies. In addition, the election official has a legitimate reason to be in contact with these machines while tabulation is ongoing in order to carry out such attacks. Despite this possibility, these attacks are barely viable on the individual level, and infeasible at scale. The quantity of ballots central ballot scanners can process is too large for an election official to have a significant effect manually sorting or editing the scanned ballots.

Interestingly, hacking the ballot definition as is described in attack 4 above but targeting the ES&S DS850 BFOS could have a higher likelihood of success. This is because the DS850 is able to sort ballots into separate trays as they are output [34]. With the security measures in most tabulating facilities, and the presence of poll watchers [35] attacks such as these which require modification of the paper trail are not generally viable.

A DoS attack against a central ballot scanner would be drastically more difficult to execute than one against a HFOS. Fewer participants in an election are permitted to be in contact with the HFOS, narrowing the set of suspects. In addition, central scanning locations have multiple scanners the majority of which would need to be disabled to significantly disrupt an election. As well, some locations have poll watchers [35], making it impossible for an attacker disabling multiple machines to go unnoticed.

For these reasons, while there are vulnerabilities with at least some existing BFOS, the risk of these being exploited for the large scale modification of an election is minimal in the presence of best practices, namely poll watchers and RLAs.

3.4 Ballot Marking Devices

US elections use BMDs in some polling places to allow voters to mark their ballot using push buttons or on a screen, and receive a printed, marked paper ballot from the BMD. Sometimes, BMDs include the ability to print out a "ballot summary card" [36], summarizing the votes cast using that machine during the election. Given that it is sometimes easier and quicker for a voter to complete their paper ballot by hand, BMDs are frequently used for enhancing election accessibility, permitting those who are unwilling or unable to fill out a paper ballot to mark one. Nevertheless, these machines are not solely used for accessibility, some localities mandate the use of BMDs for all voters [15, 21, 36, 37].

3.4.1 Threat Model

Voters, poll workers and election officials come into contact with BMDs as part of the normal course of an election. The threat model must therefore consider these three individuals as possible attackers [36–38].

- A voter comes into contact with the BMD through normal participation in an election in jurisdictions which use these machines for all or some in-person voters [15].

- A poll worker has direct, legitimate contact with BMDs as they are tasked with configuring these systems for elections. As such, poll workers have the ability to access the administrative interfaces of BMDs in order to program these machines for upcoming elections and aggregate the results of those elections [38].

- Election officials have the privileges of a poll worker, and the ability to access these machines while they are in storage [6].

3.4.2 Vulnerabilities

Attendees at the DefCon 27 Voting Machine Hacking Village attempted to hack the ES&S AutoMARK. Through this

engagement, researchers found the AutoMARK system to be insecure against an attacker with physical access to the machine. Researchers found physical security controls to be lacking: the lock protecting the data drive on the system was easily picked, and an RJ-45 port on the front of the ES&S AutoMARK machine was accessed which was obscured by an easily-removed sticker[20]. The Windows CE operating system was significantly outdated, having last been updated in 2007. This operating system has at least two CVEs against it [40] and was also discovered to have non-critical software such as Internet Explorer installed increasing the AutoMARK's attack surface. Researchers modified the "load address"[21] [4] causing the BMD to crash repeatedly. Furthermore, the password needed to change the firmware was the default value "1111" [4]. The administrator password was able to be extracted in plain text from configuration files which permitted attackers to enter administrator mode on the machine [4, 36].

3.4.3 Implications

When examined together, these vulnerabilities jeopardize the security of the AutoMARK BMD with relation to multiple attacker goals outlined in Section 2.3.2. We assert that an attacker could achieve any of the following attacks based on the vulnerabilities outlined above:

1. By gaining remote code execution on the device through any method (CVEs, other outdated software vulnerabilities, physical access to storage card or RJ-45 port, malicious firmware installation, access to administration panel), an attacker could alter the load address causing the BMD to crash repeatedly. This would achieve Attack 3, and would be challenging for a non-technical election official to discover and remedy. A voter would be unlikely to be able to execute this attack, as it would require the voter to be prepared and interact with the machine for an extended period of time. Election officials and poll workers alike, however, have prolonged contact with the administrative interface of the machine, facilitating this attack.

2. A voter (or poll worker or election official) could rapidly open the enclosure for the data disk and removing the disk, an attack we speculate will take the machine out of commission. This constitutes a successful DoS attack (Attack 3).

3. A voter, poll worker or election official with a specially crafted device and payload could connect to the exposed RJ-45 port and exploit a known CVE against Windows CE Embedded 5.0 which would permit them to perform a DoS [40]. This would accomplish Attack 3.

4. A poll worker or election official could use their access to the machine to install a malicious program which alters votes between the time they are entered and printed. The results of this attack could be a discrepancy between the printed ballot and the ballot summary card (if equipped), or a discrepancy between the voter's selections and both printed outputs of a BMD. Given that most voters do not inspect either their paper ballot or the ballot summary card[22], this attack method could subtly alter votes by misprinting ballots. Remedying this attack is tougher than it may seem. As a direct consequence of the fact that neither paper trail (printed ballot nor ballot summary card) can be declared to be authoritative as they are both printed by the same system, a conflict between these two is impossible to optimally resolve when caught at audit-time [36]. If this attack were to succeed in altering votes, this would constitute completion of Attack 1.

5. Any of the aforementioned attacks (1, 2, 3, and 4) would serve, if publicly disclosed, to undermine the confidence in elections, inadvertently or expressly achieving Attack 2.

The functioning of most BMDs is simple and similar to one another. There is no reason to believe that similar attacks are not present on other machines of this type including those listed in Table 1.

Such attacks pose a significant risk, even with the presence of RLAs. To vote on a BMD, a voter must check that their ballot has been printed as they voted, sometimes involving verifying their selection on many races. An attacker subtly modifying a small percentage of ballots on a smaller race would likely go unnoticed. In the event that a user identifies that a ballot has been modified, they will simply recast their vote, blame human or machine error, and the malware would leave the ballot unmodified. Moreover, if an attacker can successfully modify ballots or the ballot summary card, they can create a discrepancy which is difficult to resolve as it requires considering the printed ballot or ballot summary card authoritative. These issues add to numerous others issues with BMDs[23] to frame BMDs as an imperfect solution, especially when compared to the authoritative HMPB [36].

While we have presented a selection of plausible vote-changing and DoS attacks, these attacks are difficult to execute during an election across many machines. It is equally unlikely that an election official is able to execute such attacks at scale without raising suspicion. Therefore, these attacks are unlikely to modify a large election, and will require a significant amount of work to alter a smaller election. Even then,

[20] It appears that the purpose of this sticker is to be tamper evident [39]. It is unclear whether this sticker was such a seal.

[21] Presumably the load address of the binary used to run the capabilities of the BMD.

[22] Ballot summary cards and ballots are sometimes difficult to read as a result of their use of bar codes, QR codes and small font. Voters do not often put in the effort to check these, especially if the systems complicate the checking process [36]. Additionally, it is not clear what fraction of voters have the ability to view the ballot summary card at all.

[23] See [36] for more information.

BMDs represent a small fraction of the ways in which voters mark their ballots, with HMPB making up significantly more. Therefore, targeting these machines is not ideal for an attacker wishing to modify the outcome of a large election [21].

3.5 Direct Recording Electronic

DREs have seen increase use in polling places as a result of HAVA which sought to replace the allegedly fallible punch card machines of the 2000 presidential election. Elections employ these machines to simplify how users vote by making a selection on the screen, after which the vote is tabulated to onboard storage within the DRE. When the election closes, poll workers aggregate the tallies from all DREs used in a precinct to form the results of the election. To heed warnings issued by researchers about the dangers of casting, recording and tallying votes on the same machine without a paper trail [20], manufacturers of DREs began including Voter Verified Paper Audit Trail (VVPAT) as a stopgap solution. VVPAT consists of the voter's selection printed onto receipt paper behind a glass window on a DRE. Ideally, a voter compares their vote as cast with the most recent entry on the tape [1, 6, 15, 19, 41–44].

3.5.1 Threat Model

An attacker may assess that, given the fully computerized nature of a DRE, this sort of machine should be targeted to carry out malicious actions against an election. This conviction is founded as the reliance on a computer makes DREs vulnerable to cyber attacks, while the paper trail (VVPAT) is only present on some designs, and is not as authoritative as a HMPB. In order to evaluate the security of DREs – systems which come in contact with voters, poll workers and election officials in an election – we must consider the following attackers as the threat model against this machine.

- A voter comes into contact with the DRE through their participation in an election in a jurisdiction which uses DREs for in-person voters. This contact does not usually last for an extended period of time, however voters are granted privacy while voting [6, 15, 41, 43].
- A poll worker has direct, legitimate contact with DREs. Poll workers are tasked with configuring and deploying the DRE for elections and tallying the results at the end. Both of these actions require they interact with the administrative interface of the machine [6].
- Election officials have the privileges of a poll worker as well as the ability to access these machines while they are in storage [6].

3.5.2 Vulnerabilities

The Diebold AccuVote TSX has been publicly audited at the DefCon 26 Voting Machine Hacking Village, where researchers discovered significant flaws in the machine. In addition, a 2007 paper found severe issues in the AccuVote TS, a very similar device to the TSX [3, 7]. We will consider both here to highlight vulnerabilities against the DRE class of voting machine.

When examining the AccuVote TS, researchers injected malware by replacing the bootloader which required exploiting a backdoor in Diebold code which checks for the presence of certain files on the memory card in order to boot the operating system into Windows Explorer. From Windows Explorer, researchers achieved arbitrary code execution. As an alternative route to injecting malware, researchers were also able to execute their payload by replacing the factory EPROM memory chip with a maliciously crafted one. In addition, researchers found that based on the presence of a single file on the memory card, the machine will erase the filesystem and flash data. To demonstrate the impact of these vulnerabilities, researchers developed successful attacks against this machine which achieved vote stealing (Attack 1) and DoS (Attack 3) [7].

During DefCon, researchers stole[24] a mock election implemented on a AccuVote TSX DRE. During this race, the two candidates (George Washington and Benedict Arnold) both lost to Jeff Moss, a candidate not available for selection on the ballot of the special election. In addition, the election configuration used in the attack was crafted by researchers without use of proprietary software which would be used by election officials for this purpose. Furthermore, attendees recreated previous attacks including picking the lock to access the power button with a ballpoint pen, and accessing the administrative interface by simply removing the card reader from the machine before bootup [3].

3.5.3 Bypassing VVPAT

Though the fundamental idea behind VVPAT – that of necessitating a paper trail – is a crucial point for ensuring elections are auditable, VVPAT as implemented does not perfectly address the problem. This happens for many of the same reasons as the computer-generated paper trail of a BMD (as described in Section 3.4.3) falls short. Some of the issues raised with VVPAT include small font on the VVPAT tape, window covering the VVPAT tape for privacy [41], and voters being uninformed about the purpose of the VVPAT tape and possibly not checking their cast vote against the tape. Even if a voter is to check their entry on the VVPAT tape, they are often voting in multiple races, so it may be hard to remember how they voted for each [42, 45].

[24] Stealing an election is to alter votes in a race in order to change the outcome to one preferable to the attacker.

To highlight the shortcomings of VVPAT, we demonstrate that all an attacker needs to do to compromise a DRE with VVPAT is to design the malicious code such that it does not stuff every vote cast. When the malware chooses to alter a vote, it does so both in the stored ballot in memory and onto the VVPAT tape. If this alteration is detected by the voter, election officials will remove that vote from the tally and prompt the user to re-submit their vote. This time, the malware will not alter the cast vote, and the voter will see what they expect on the VVPAT tape. This makes it very hard to detect that a malicious program is in control of the system, as these sorts of errors could be attributed to computer glitches or user error [45].

Of course, it follows from these attacks that an attacker could compose a malicious program which would simply stuff the VVPAT tape and the tallied ballot count with as many votes for whichever party they desire. Needless to say, this attack method is much more evident if the targeted election is audited. Both of these attacks on VVPAT would have the effect of altering the count of the election, achieving Attack 1.

3.5.4 Implications

In addition to the attacks against VVPAT listed above, DREs offer more avenues of attack than this. We list these below:

1. A DoS attack against a DRE could take advantage of the lacking physical security controls on these machines. As demonstrated through all of the research pieces examined, physical access to these machines is enough to perform a DoS attack against these machines for a significant period of time in a variety of ways [3, 6, 7]. More complicated (and less destructive attacks) are also possible, though not necessary in order to complete Attack 3 [8].

2. Physical access to DREs can also grant a voter, poll worker or election official access to the administrative menu of the machine, permitting more advanced attacks with the goal of altering election results (Attack 1) [3].

3. It has been supposed (albeit never demonstrated) that a motivated attacker could use the VVPAT tape to deanonymize voters, which would complete Attack 4. This is hypothesized to be possible if a poll-watcher is able to collect an ordered list (of names or other identifying information) of voters on election day, and compare this with the order of votes on the VVPAT tape to determine how voters cast their votes. There is not any evidence of such attacks actually taking place or being practical to perform [45].

4. DREs without VVPAT (5.8%[25] as of 2022) are easier targets for malicious actors than systems with VVPAT. The complex attacks outlined above and in Section 3.5.3 can be simplified, as the attacker or malware is not concerned with having to match the modified tallies with a VVPAT tape. The lack of a paper trail makes these machines hard if not impossible to audit[26]. Therefore, all an attacker would need to alter ballot counts undetected on a machine without VVPAT is arbitrary code execution and a knowledge of the tallying software [3, 7]. This attack highlights why DREs without VVPAT are considered among the most dangerous systems in elections today [42]. Modifying these VVPAT-less DREs is a perfect approach to achieving Attack 1 undetected.

5. If implemented and detected and publicized, these attacks (1, 2, 3, and 4 above and those presented in Section 3.5.3) can have the direct effect of achieving Attack 2. Public confidence in elections can be easily reduced by sharing evidence of such attacks taking place.

The vulnerabilities outlined above allow us to surmise that the Diebold AccuVote TS and TSX are acutely vulnerable to an attacker with physical access. This danger is only compounded with the increased legitimacy and duration of interaction with the system as would be expected of a poll worker or election official. Indeed, with adequate time, any of these attackers could succeed in executing Attacks 1 and 3, causing Attack 2 to follow from either.

Given research into other systems such as coverage of the vulnerabilities in the ES&S iVotronic in [6] and [5], there is reason to believe that similar attacks are present across most or all DRE equipment, including those referenced in Table 1. These attacks are especially severe and difficult to recover from, especially in the case of DREs without VVPAT. DREs, and most notably those without VVPAT, represent the easiest targets for an attacker wishing to modify votes undetected. It is for this reason that the election security community have concluded that these machines are the biggest threat to the US election system in its present state [42].

3.6 Networking and Voting Machines

The discussion of vulnerabilities in the networking software or concerning the exposed RJ-45 ports of certain machines raises the question of how voting machines use networking. There are two types of networking that apply. Machines are commonly networked on internal networks [6, 14, 46] and sometimes to the wider internet[27] [2]. With each comes risk, as detailed below.

[25] Percentage of registered voters living in jurisdictions using Direct Recording Electronic (DRE) Systems without VVPAT for all voters [21].

[26] The only possible auditing would be forensic auditing of the machines post-election to determine the presence of malicious software.

[27] Sometimes inadvertently.

3.6.1 Internal Network Connectivity

It is common to see an RJ-45 port on voting machines. In some configurations, election officials can use this port to network an array of machine with a central server to manage the machines and aggregate the data from each [14, 46]. This endangers each machine with a trusted link to the central computer: if an attacker is able to access the software which controls the election centrally[28], they can spread virally through the network, attacking all the hosts on the network as one. An attacker can use the management software to their advantage in achieving this [6].

3.6.2 External Network (Internet) Connectivity

Connectivity of voting systems to the internet is widely considered a dangerous procedure. Being accessible from the internet puts these systems at great risk of being attacked, as it is common practice for adversaries to attempt to attack election infrastructure, and directly connecting these devices to the internet facilitates this. Even systems outside the election industry which are kept relatively up to date are regularly targeted and exploited. All of the examined voting machines to date do not nearly meet the level of upkeep that the rest of the systems on the internet receive, and therefore, voting machines connected to the internet are at higher risk from malicious actors [2].

3.7 Trust in Elections

In the current US election scheme, great trust is placed in the hands of election operators. Realistically, despite attempts to decentralize elections as discussed in Section 4.1, the election process and election operators are inextricably tied.

This trust in elections is used to fill the gaps where the current US system does not meet the requirements for an ideal election as set out in Section 2.2. For example, where the current system generally falls short in verifiability, voters place trust in election officials to carry out audits and recounts as well as to accurately configure machines in order to ensure that a voter's vote is tallied and recorded as it was cast.

3.8 Summary

We have established that regardless of manufacturer or machine type, all examined computerized election machines have been found to be vulnerable to some attacks. These vulnerabilities represent an inevitability when dealing with computer controlled systems. This demonstrates the importance of a properly formed paper trail. Physical security measures combined with the millions of ballots used in a national election make tampering with the paper medium more difficult than its software counterpart. This necessity for a reliable paper trail is no more evident than when comparing a HFOS to a DRE, as shown in Table 2. Despite not being significantly different in exposure to vulnerabilities, the HFOS produces an authoritative paper trail which can be used to recount the election manually and derive an exact count, nullifying the risks of most of these vulnerabilities. Comparatively, recounts to address tampering of a DRE (assumed to be without VVPAT) must rerun the election completely [15]. Even in the presence of VVPAT (or ballot summary cards for DREs), the paper trail generated by a computer requires voters to check their votes tediously, and does not provide an authoritative paper trail [45]. Therefore, we assert that an authoritative paper trail is the best way to safeguard elections taking place on computer-driven election machines for the foreseeable future.

Another conclusion from this examination of the current state of election machines is an immediate need for auditing of all elections. Trusting machines that have been shown to have countless vulnerabilities puts elections in jeopardy, most pressingly in cases where those machines do not have a paper trail. Applying RLAs to all elections passed through any computerized machine is therefore a necessity. Regardless of the attack method, if it has the Attack 1 goal of modifying election outcomes, an RLA can detect it and set in motion the appropriate recounts or other remediation measures. [47].

4 Proposed Future Scheme Examinations

As stagnant as the current selection of election equipment might seem at any given moment, the truth is that on a broad scale, election systems are replaced and altered continually [19]. This has led to a multitude of proposed designs for new voting machines. Among these proposals, an eagerness to use cutting edge technology is inevitable. From schemes which suggest using blockchain to designs aimed at taking advantage of novel cryptographic techniques and formal programming practices, these candidate election technologies present a wide range of innovative approaches to a difficult problem.

In this section, we examine two possible technological responses to the challenging question of elections. For each, we have chosen a scheme that has yet to piloted in a real election, and represents an adequate application of the underlying technology to elections. Based on this, we question whether:

- The design adequately addresses the requirements for a successful election, outlined in Section 2.2.
- The design is secure against attacks set out in Section 2.3.2.
- The design does not repeat any of the shortcomings of past and present election systems (described throughout Section 3).

[28] In the case of ES&S products, this software is called Unity.

Election Scheme	Privacy Requirements			Verifiability Requirements		
	Ballot Secrecy	Receipt-Freeness	Coercion-Resistance	Cast-as-Intended	Recorded-as-Cast	Tallied-as-Recorded
Blockchain Solution by Ayed [12]	Fail	–	Fail	Fail	Pass	Pass
Microsoft ElectionGuard [13]	Pass	Pass	Pass	Pass	Pass	Pass

Table 3: Evaluation of blockchain voting solution proposed by Ayed in [12] and ElectionGuard proposed by the ElectionGuard team in [13] against the six major requirements for an election as defined in Section 2.2.

Election Scheme	Attacks			
	Attack 1	Attack 2	Attack 3	Attack 4
Blockchain Solution by Ayed [12]	Vuln.	Vuln.	Vuln.	Vuln.
Microsoft ElectionGuard [13]	Safe	Vuln.	Safe	Safe

Table 4: Evaluation of blockchain voting solution proposed by Ayed in [12] and ElectionGuard proposed by the ElectionGuard team in [13] against the four attacks against election schemes described in Section 2.3.2.

4.1 Blockchain-Based Election Scheme

The rise of cryptocurrency has brought the term *blockchain* into the public lexicon. A blockchain is a cryptographic construction which relies on each participant storing a copy the public dataset (in the case of cryptocurrencies, a ledger) on their device. This makes blockchains decentralized – meaning they do not rely on a central server [25, 48].

As discussed in Section 3.7, one of the major shortcomings of elections in the US today is the requirement that to trust an election, a voter must trust the officials that run it. For this reason, academics and corporations alike have sought to capitalize on this decentralized architecture by using it to create voting methods with more verifiability [24]. Proponents of blockchain cite additional benefits of using blockchain for elections. For one, verifiability is usually trivial when each voter holds a copy of the set of all ballots. Moreover, assuming blockchain-based voting technologies eventually become dominant, some proposed solutions claim this move to digital voting will make voting more accessible and commensurately increase the notably low US voter turnout [9, 48].

Despite the enthusiasm towards adopting solutions for elections based on blockchain, the attempts to apply blockchain to elections have to date produced products which do not meet the requirements of an election. Some of these proposed solutions have even been shown to be highly insecure when audited after being piloted in real elections or polls [10, 24, 49].

4.1.1 Suggested Technology

The choice to review the solution proposed by Ayed [12] and shown in Figure 1 was made by examining the most cited works for the Google Scholar query "blockchain voting". Of the most cited results, Ayed and a piece by Hjálmarsson et al. [25] were the two which proposed actual implementations of election systems using blockchains. Despite being a more complete description of the implementation, Hjálmarsson et al. advocated for a concept of "liquid democracy" [25] which makes it unfit to consider against the requirements of US elections.

Though the description of the scheme is brief, Ayed offers a description of a design for a public blockchain-based election scheme. In this proposed scheme, Ayed establishes the target election requirements of authentication, anonymity, accuracy and verifiability. The phrasing of the requirement of anonymity does not explicitly include the requirement of Coercion-Resistance from Section 2.2, instead focusing on the property that there should be no link between the voter and ballot.

The structure of the blockchain Ayed proposes is based on an initial transaction with the name of the candidate placed on a separate blockchain for each candidate. Subsequently, each vote for that candidate will be passed to a node (one of which will be in each "district" [12], to ensure that the system remains 'decentralized'), and that node will register the vote onto the blockchain corresponding to the voter's choice. The header of the block which the node commits to the blockchain will feature a hash of the user's unique voter ID number, user's full name and hash of the previous block in the blockchain, hashed using a secure hashing algorithm.

Tallying of the votes, as well as verification of the count, can be performed by any interested party by counting the number of blocks committed to the blockchain attached to the source block containing a candidate's name.

4.1.2 Evaluation

To evaluate this proposed election scheme, we evaluated the scheme proposed by Ayed [12] against the requirements for an ideal election as set out in Section 2.2. A summary of these results is presented in Table 3. If applicable, attacks are associated with an attacker goal in Section 2.3.2 and the vulnerability of this scheme is presented in Table 4.

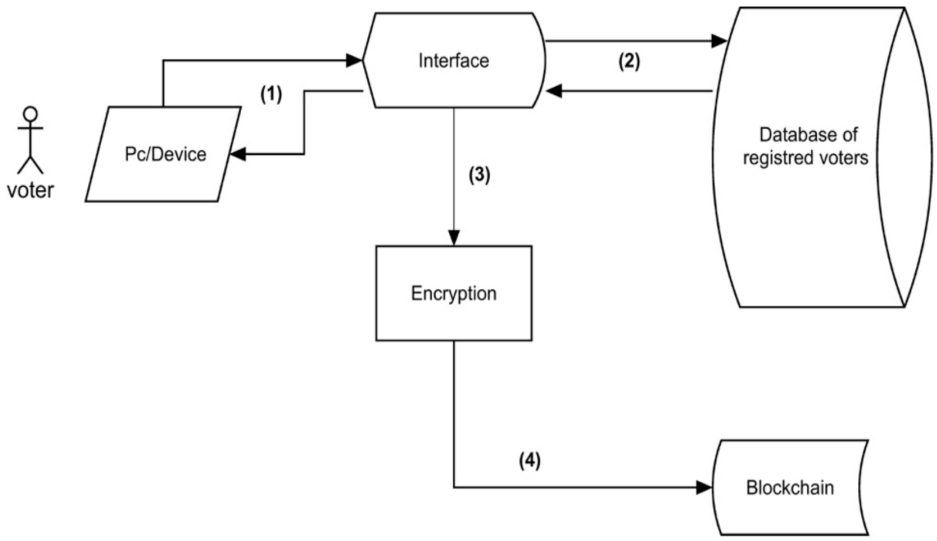

Figure 1: Blockchain voting scheme as designed by Ayed [12].

Privacy: Ballot Secrecy: Fail: For a determined attacker, this voting solution does not guarantee Ballot Secrecy. An attacker can use the timing of a ballot's casting as perceived in network traffic to pinpoint the ballot in the blockchain and identify the candidate for which the target voter cast their ballot. Should an attacker be able to attain this data, they would succeed at Attack 4.

Privacy: Receipt-Freeness: N/A: This scheme omits any provision for providing a voter a receipt.

Privacy: Coercion-Resistance: Fail: While we have shown above how an attacker can determine a voter's vote using timing and could thereby coerce the voter to vote in a certain manner, we identified other ways that a voter could be coerced into proving that they voted a certain way. This digital election scheme takes place on a computer, and in much the same way as current-day voting can be coerced by the voter taking a video of themselves casting their vote, this scheme leaves room for the voter to record their screen as they submit their ballot to prove to a malicious actor that they voted a certain way. Moreover, a voter can be pressured to supply their voter ID number and full name to a malicious actor who may then search through all cast votes, testing the header of each vote (using the hash of the last block as the third input for checking whether the current block is the coerced voter's vote) in order to locate the vote of the coerced voter and determine how they cast their vote.

Verifiability: Cast-as-intended: Fail: There is no proof to the user that their ballot has been cast (in this case, sent to the node for processing).

Verifiability: Recorded-as-cast: Pass: Presumably, the voter has access to the hash of the previous block in the blockchain[29]. This would permit the voter to identify their vote in the blockchain by recalculating the hash which makes up the block header of their ballot and locating the corresponding block on the blockchain, ensuring it is cast for the right candidate.

Verifiability: Tallied-as-recorded: Pass: In this scheme, any voter can tally votes cast for each candidate as the blockchain is public. This permits any voter to locate their ballot (as stated above) and tally the election, knowledgeable that this count includes their ballot.

Though this scheme represents a rather simplified attempt at constructing a blockchain election scheme, we have shown that it does not uphold several of the requirements of an ideal US election. Furthermore, there are a multitude of issues with this scheme, some of which are listed below:

- This scheme suggests using a blockchain for each candidate in each race. Some races have several candidates or ballot measures, raising the number of blockchains that each participant in the blockchain would need to store.
- There is no ability to audit the functioning of the scheme externally. If an adversary could access a "node" [12] (the computer responsible with committing blocks (votes) to the blockchain) they could add an arbitrary number of votes to the candidate of their

[29]This is not required to locate a ballot, merely useful to have in order to reduce time it would take to search the blockchain. The search algorithm would only have to compare hashes rather than calculate then compare hashes for each vote.

choice. Further, if detected post-election (for example if the adversary committed more votes than there were total registered voters), there is no recourse for remediation. A rerun of this election would be unable to prevent this same attack from occurring again. An attacker could succeed in Attack 1 by taking advantage of this flaw. Another result of achieving control over a node could be a partial or complete DoS attack against the scheme, resulting in Attack 3. Either of these attacks, if revealed to the public, would reduce voter confidence in the security of the "nodes" [12] and by consequence the scheme itself. This would result in successful completion of Attack 2.

- Despite claiming to be a decentralized system, this implementation relies heavily on precinct-based nodes. These nodes possess more ability to sway an election than their current analog, the central ballot scanner.
- As with any digital voting scheme, the endpoint machines users use to cast their votes are susceptible to malware which could seek to alter the cast vote or expose the voter's vote. This could allow an adversary a limited ability to achieve Attack 1. Another form of malware could record and disclose how a voter voted, resulting in Attack 4.
- Being a distributed system, reliant on a large set of parties running an application and possessing portions of the blockchain, it is difficult to update all clients, even when the update patches a vulnerability [10].
- Blockchain is not a new technology, but modern implementations of this technology are still in early stages of development. It is common for researchers to find and disclose vulnerabilities in all components of blockchain technology. Therefore, this technology – as with any cutting edge technology like it – should not be immediately brought to bear on critical infrastructure such as elections, rather testing throughout industry should occur first [10].

In summary, this simple blockchain-based election scheme demonstrates several fundamental issues. These issues highlight how, while blockchain technology has use in the distributed finance sector, blockchain technology is not optimally suited to being applied to elections. Perhaps blockchains will see use as one part in a larger election scheme, however using the blockchain to vote, as evidenced by the analysis of Ayed's proposed scheme, is not an optimal solution for conducting elections [48].

4.2 Non-Blockchain E2E Verifiable Election Scheme

Excluding blockchain-based solutions when examining how cutting edge technology is applied to elections, other E2E verifiable election schemes stand out. These schemes aim to meet the requirement of being E2E verifiable – permitting all voters to independently verify the steps an election, as described in Section 2.2. In this section, we focus on schemes which use other novel approaches to solve the complex set of requirements of an election.

4.2.1 Suggested Technology

We made the choice to review the solution proposed by the ElectionGuard team in [13] and shown in Figure 2 as this system is at the intersection of cutting edge cryptography and E2E verifiability. Furthermore, it appears to be the most developed solution employing these technologies which has not been realized and trialed in a real election.

ElectionGuard makes claims as to what requirements of an election it upholds. In a blog post about ElectionGuard on the Microsoft Blog, ElectionGuard claims to be verifiable, permitting a voter to ensure that their vote was among the set of all votes, and that this set of votes was properly tallied [50]. In a separate blog post, ElectionGuard claims to uphold the principle of Ballot Secrecy and Coercion-Resistance [23].

The intended use-case for ElectionGuard is as an SDK for supplementing or designing E2E verifiable elections. Despite this, the online documentation contains a reasonably complete description of how to conduct an election primarily using ElectionGuard [13].

The first step of this election using ElectionGuard is to define the election parameters. Among these parameters is the minimum required number of election encryption key "Guardians" [13] (election officials who hold fractional keys to the election) present at decryption time. Then, the Guardians define the election encryption keys and provide a fractional key to each Guardian. This process distributes the election decryption key among the Guardians, and sets the attendance threshold for decrypting the election once complete.

After this, the election commences, and voters cast their ballots. These ballots are either cast or spoiled[30] by the voter.

Once the election completes, the set of all encrypted ballots and corresponding proofs ensuring ballots have not been altered are published online. ElectionGuard combines all cast ballots using homomorphic encryption to generate an encrypted tally of the election. The Guardians of election encryption keys gather. Assuming the number of guardians present is greater than or equal to the required minimum number set during the key ceremony at the beginning of the election, they decrypt the homomorphically tallied results and publish this result along with all other important election files. A curious voter, or other third party can verify the election using this published data and corresponding tools. Organizations or individuals can also compose their own tools to perform this verification [13].

[30] Also referred to as challenging a ballot. [13]

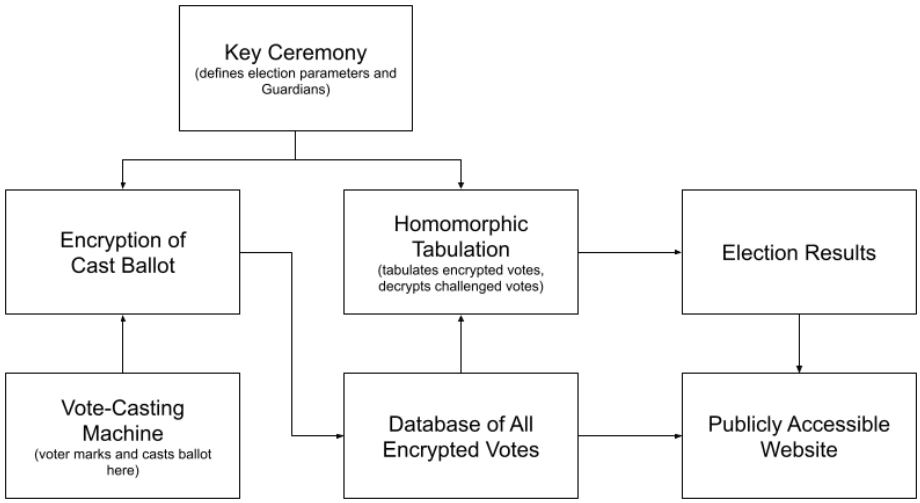

Figure 2: Example ElectionGuard workflow as designed by the ElectionGuard team [13].

4.2.2 Evaluation

To evaluate this proposed election scheme, we evaluated the solution proposed by the ElectionGuard team in [13] against the conditions of a perfect election as set out in Section 2.2. A summary of these results is presented in Table 3. If applicable, attacks are associated with an attacker goal in Section 2.3.2 and the vulnerability of this scheme is presented in Table 4.

Privacy: Ballot Secrecy: Pass: ElectionGuard encrypts each ballot using ElGamal encryption from the moment it is cast [13]. Only spoiled ballots are decrypted after the election has concluded. This maintains Ballot-Secrecy.

Privacy: Receipt-Freeness: Pass: ElectionGuard provides voters with a tracking code devoid of information that can link them to their vote. This fulfills the requirement of Receipt-Freeness as it does not reveal the voter's choice while providing a receipt [13, 23].

Privacy: Coercion-Resistance: Pass: ElectionGuard takes place on a computer, and in much the same way as current-day voting can be coerced by the voter taking a video of themselves casting their vote, this scheme would allow the voter to record their screen as they submit their ballot to prove to a malicious actor that they voted a certain way. Given that ElectionGuard is absent of additional methods of violating Coercion-Resistance, we consider this a pass, as it is not feasible to extricate this method of coercion from any feasible election system.

Verifiability: Cast-as-intended: Pass: The user can verify that their encrypted ballot has not been modified since it was cast using their tracking code they receive as a receipt after casting their vote [23].

Verifiability: Recorded-as-cast: Pass: Proofs provided alongside the published set of all encrypted ballots and the tracking code provide the user with confirmation that their ballot has not been tampered with between the time it was cast and when it is recorded [23].

Verifiability: Tallied-as-recorded: Pass: Given that ElectionGuard provides all election data as well as a verification program to check that the results were correctly tallied, this system allows the user to verify the tally counts all ballots as they were recorded [13, 23, 50].

Should homomorphic-encryption-based E2E election systems see use in the US, they will not look exactly like ElectionGuard. However, it is possible to point out a couple shortcomings in election systems like ElectionGuard in hopes that these will be addressed in any publicly deployed system. Some of these are as follows:

- ElectionGuard relies on election officials ("Guardians" [13]) to hold the keys to the election. Therefore, there still remains[31] a required element of trust in these officials on behalf of the voters [51].
- Given the complexity and novelty of ElectionGuard, it is essential that election workers be well trained to perform the tasks needed to run the election. In the event of a partial or complete failure of this highly technical system, expertise must be available to make sense of the issue an communicate to voters what has occurred in simple language [51].

[31] See Section 3.7

- Being innately technical, ElectionGuard (and most E2E verified schemes) will require a delicate handling when presented to voters. Specifications and encryption methods are useful terms within computer science, but to explain E2E verified elections and homomorphic encryption to a lay-audience and engender trust in the election system within that audience, the topic must be carefully presented [24]. Failure to properly inform voters as to the functioning of ElectionGuard could facilitate the successful dissemination of misinformation aimed at undermining voter trust in the system. This would accomplish Attack 2.

- ElectionGuard pairs E2E verification with a cutting edge cryptographic technology for operating on encrypted datasets – homomorphic encryption. This is another technology that has yet to see widespread industry use, and experience the amelioration in reliability and understanding associated with such use. Therefore, while a promising and well-informed proposal for an E2E verifiable voting scheme, ElectionGuard and similar schemes should be resigned to testing until confidence is gained in the trustworthiness and reliability of their underlying technologies [10].

While ElectionGuard fully satisfies the election requirements on paper, it has yet to see real-world testing. Though other E2E verified schemes have been piloted or implemented around the world, E2E verification is still in its infancy, and will require prolonged real-world experience in order to gain a good track record [24]. In the long term, once the underlying technologies have seen adequate experimentation in industry, ElectionGuard as well as other E2E verified election schemes hold great potential for positively impacting US elections.

5 Conclusion

In this paper, we presented the machines currently used in US elections and selected flaws in these machines. Subsequently, we examined novel schemes against the requirements of an ideal election, an noted where those schemes fell short of the requirements. The main conclusions of this work are twofold. Firstly, though at a glance there is evidence that the current election system is vulnerable, the safeguards in place diminish this threat significantly. Secondly, we have established that an election's ability to thwart tampering relies on a relentlessly audited authoritative paper trail. In future schemes, we recommend that this auditability not be ignored, as it provides a tangible manner in which everyday voters can experience greater trust their elections.

Acknowledgments

We acknowledge the efforts of Dr. Yeongjin Jang in reviewing and mentoring this project. We also acknowledge Dr. Stuart Read for reviewing this paper. Lastly, we acknowledge the participants and organizers of DefCon Voting Machine Hacking Village for facilitating unparalleled open research into the flaws in election systems.

References

[1] K. Zetter, "Fixing democracy: The election security crisis and solutions for mending it," *Texas National Security Review*, vol. 3, no. 4, p. 102–111, 2020.

[2] National Election Defense Coalition, "Internet connectivity in voting machines." https://www.electiondefense.org/internet-connectivity-in-voting-machines.

[3] M. Blaze, J. Braun, H. Hursti, D. Jefferson, M. MacAlpine, and J. Moss, "Defcon 26 voting village report." https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf, Sep 2018.

[4] M. Blaze, H. Hursti, M. MacAlpine, M. Hanley, J. Moss, R. Wehr, K. Spencer, and C. Ferris, "Defcon 27 voting machine hacking village report." https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf, Aug 2019.

[5] A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze, "Security evaluation of es&s voting machines and election management system." https://www.usenix.org/legacy/events/evt08/tech/full_papers/aviv/aviv.pdf, 01 2008.

[6] P. McDaniel, K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, M. Blaze, A. Aviv, P. Černý, S. Clark, E. Cronin, G. Shah, M. Sherr, G. Vigna, R. Kemmerer, D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, W. Robertson, F. Valeur, J. L. Hall, and L. Quilter, "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing." https://www.eac.gov/sites/default/files/document_library/files/EVEREST.pdf, 2007.

[7] A. J. Feldman, J. A. Halderman, and E. W. Felten, "Security analysis of the diebold accuvote-ts voting machine." https://citp.princeton.edu/our-work/voting/, 2006.

[8] HackerHouse, "Diebold accuvote-tsx election machine hacking." https://hacker.house/lab/hacking-

elections-diebold-accuvote-tsx-runs-space-invaders/, Oct 2019.

[9] P. Lam, "From helios to voatz: Blockchain voting and the vulnerabilities it opens for the future." https://www.cs.tufts.edu/comp/116/archive/fall2019/plam.pdf, 2019.

[10] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: from internet voting to blockchain voting," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyaa025, 2021.

[11] D. S. Wallach, "Security and reliability of webb county's es&s voting system and the march '06 primary election," *Accurate*, May 2006.

[12] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.

[13] ElectionGuard Team, "What is electionguard?." https://www.electionguard.vote/.

[14] Election Systems & Software, "Es&s model 650 central ballot scanner operator's manual." https://verifiedvoting.org/wp-content/uploads/2020/08/M650-OM-v.-2.1_12.15.2005.pdf.

[15] Verified Voting, "Voting equipment." https://verifiedvoting.org/votingequipment/.

[16] J. H. Myers, "Voting machine." https://votingmachines.procon.org/wp-content/uploads/sites/46/levermachinepatent.pdf, U.S. Patent 415 549, Nov. 1889.

[17] ProCon.org, "Historical timeline: Electronic voting machines and related voting technology." https://votingmachines.procon.org/historical-timeline/, Mar 2017.

[18] McKay et al., "Electronic voting machine." https://votingmachines.procon.org/wp-content/uploads/sites/46/dre.pdf, U.S. Patent 3 793 505, Feb. 1974.

[19] MIT Election Data + Science Lab, "Voting technology." https://electionlab.mit.edu/research/voting-technology.

[20] R. M. Alvarez, S. Ansolabehere, E. Antonsson, J. Bruck, S. Graves, T. Palfrey, R. Rivest, T. Selker, A. Slocum, and C. Stewart, "Voting - what is, what could be." https://vote.caltech.edu/reports/1.

[21] Verified Voting, "The verifier." https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2022.

[22] S. T. Ali and J. Murray, "An overview of end-to-end verifiable voting systems." https://arxiv.org/abs/1605.08554, 2016.

[23] A. Thornton, "What is electionguard?." https://news.microsoft.com/on-the-issues/2020/03/27/what-is-electionguard/, Mar 2022.

[24] S. Dzieduszycka-Suinat, J. Murray, J. R. Kiniry, D. M. Zimmerman, D. Wagner, P. Robinson, A. Foltzer, and S. Morina, "The future of voting: end-to-end verifiable internet voting: specification and feasibility assessment study." https://www.usvotefoundation.org/E2E-VIV, Jul 2015.

[25] F. T. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th international conference on cloud computing (CLOUD)*, pp. 983–986, IEEE, 2018.

[26] J. Dodds, "Trustworthy elections," (San Francisco, CA), USENIX Association, Jan 2020.

[27] Cybersecurity and Infrastructure Security Agency, "Election infrastructure cyber risk assessment." https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf, 2020.

[28] National Conference of State Legislatures, "Voting outside the polling place: Absentee, all-mail and other voting at home options." https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx, Mar 2022.

[29] Election Systems & Software, "Ds200." https://www.essvote.com/products/ds200/.

[30] B. E. Corley, "Pasco county optical scan faq." https://www.pascovotes.gov/Elections/Optical-Scan-FAQ.

[31] Election Systems & Software, "M650 | es&s." https://web.archive.org/web/20130128104813/http://www.essvote.com/products/1/3/tabulators/M650.

[32] Verified Voting, "Voting equipment database – es&s model 650 (and models 150 & 550)." https://verifiedvoting.org/election-system/ess-model-650/.

[33] E. Kiely and R. Rieder, "Trump's repeated false attacks on mail-in ballots." https://www.factcheck.org/2020/09/trumps-repeated-false-attacks-on-mail-in-ballots/, Sep 2020.

[34] Election Systems & Software, "Ds850." https://www.essvote.com/products/ds850/.

[35] Texas Secretary of State Elections Division, "Poll watcher's guide - secretary of state of texas." https://www.sos.state.tx.us/elections/forms/pollwatchers-guide.pdf, Jan 2022.

[36] National Election Defense Coalition, "The dangers of ballot marking devices." https://www.electiondefense.org/ballot-marking-devices.

[37] Board of Elections in the City of New York, "Using the ballot marking device (bmd)." https://vote.nyc/page/ballot-marking-device.

[38] Automark Technical Systems, LLC, "California election procedures manual for the es&s automark voter assist terminal." https://votingsystems.cdn.sos.ca.gov/vendors/ess/2005-06-16-2e-p.pdf.

[39] Commonwealth of Pennsylvania Department of State, "Report concerning the examination results of elections systems and software evs 6021 with ds200 precinct scanner, ds450 and ds850 central scanners, expressvote hw 2.1 marker and tabulator, expressvote xl tabulatir ad electionware ems." https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/ESS%20EVS%206021/EVS%206021%20Secretary%27s%20Report%20Signed%20-%20Including%20Attachments.pdf.

[40] CVEDetails.com, "Microsoft windows ce 5.0 : Security vulnerabilities." https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-1079/version_id-421638/Microsoft-Windows-Ce-5.0.html.

[41] Verified Voting, "Voting equipment database – premier election solutions (diebold) accuvote tsx." https://verifiedvoting.org/election-system/premier-diebold-dominion-accuvote-tsx/.

[42] National Election Defense Coalition, "E-voting systems put democracy at risk: Why america's voting systems are vulnerable to undetectable rigging and cyber attacks." https://www.electiondefense.org/electronic-voting-systems.

[43] National Conference of State Legislatures, "Voting equipment." https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx, Jul 2021.

[44] Congressional Research Service, "Rl33190: The direct recording electronic voting machine (dre) controversy: Faqs and misperceptions." https://crsreports.congress.gov/product/pdf/RL/RL33190/6, Mar 2007.

[45] A. Appel, "Continuous-roll vvpat under glass: An idea whose time has passed." https://freedom-to-tinker.com/2018/10/19/continuous-roll-vvpat-under-glass-an-idea-whose-time-has-passed/, Oct 2018.

[46] Maricopa County Office of Procurement Services, "Contract: Elections tabulation system (190265-rfp)." https://www.clerkofcourt.maricopa.gov/home/showpublisheddocument/2000/637441427327330000.

[47] Free & Fair, "A path to public confidence in elections." https://freeandfair.us/articles/path-to-trustworthy-elections/, Dec 2021.

[48] Free & Fair, "Blockchains and elections." https://freeandfair.us/articles/blockchains-and-elections/.

[49] M. A. Specter, J. Koppel, and D. Weitzner, "The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in U.S. federal elections," in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 1535–1553, USENIX Association, Aug 2020.

[50] T. Burt, "Protecting democratic elections through secure, verifiable voting." https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-democratic-elections-through-secure-verifiable-voting/, May 2021.

[51] P. Ryan, J. Benaloh, R. Rivest, P. Stark, V. Teague, and P. Vora, "End-to-end verifiability," *arXiv preprint arXiv: 1504.03778*, 2015.

[52] Help America Vote Act of 2002, Pub. L. No. 107-252. https://www.congress.gov/bill/107th-congress/house-bill/3295/text, 2002.

A Acronyms

In this section, we define the election-specific acronyms used throughout this paper.

BFOS: Batch-Fed Optical Scanner; voting system which scans and tallies sets of ballots.

BMD: Ballot Marking Device; voting system where the voter's vote is entered and a completed ballot is printed by the device. No tallying takes place on a BMD.

CF: Compact Flash; removable storage device specification.

CIA: Confidentiality-Integrity-Availability; information security triad which assists in assessing the effects of an attack against a target.

CISA: Cybersecurity and Infrastructure Security Agency; federal agency under the US Department of Homeland Security (DHS) tasked with protecting American digital infrastructure.

CVE: Common Vulnerabilities and Exposures; a security flaw for a piece of software which has been publicly disclosed and assigned a CVE number.

DESI: Diebold Election Systems, Inc; manufacturer of several common voting systems.

DoS: Denial of Service; an attack against a computer system in which the goal is to render that system unable to function as intended.

DRE: Direct Recording Electronic; voting machine on which a voter selects their choice and that choice is tallied immediately into onboard memory. These machines can make use of VVPAT to increase auditability. Without VVPAT, these machines do not produce a paper trail.

DVS: Dominion Voting Systems; manufacturer of several common voting systems.

E2E: End 2 (to) End verified voting; a class of voting solutions emphasizing the voter's ability to verify the election, sometimes referred to as E2E-VIV (E2E-Verifiable Internet Voting) or E2E-V (E2E-Verified).

EAC: Election Assistance Commission; commission mandated by HAVA to assist with the administration of federal elections.

ES&S: Election Systems & Software; manufacturer of several common voting systems.

HAVA: Help America Vote Act; federal law mandating (in part) replacement of punch card and lever voting machines, establishment of EAC and definition of election administration requirements [52].

HCPB: Hand Counted Paper Ballot.

HFOS: Hand-Fed Optical Scanner; scanner into which a voter or poll worker inserts ballots manually in order to be tallied.

HMPB: Hand Marked Paper Ballot.

RLA: Risk Limiting Audit; a post election audit which uses statistical analysis to determine the likelihood of an election or tabulation being incorrect based on an examination of a small subset of cast ballots.

SDK: Software Development Kit; set of tools used to aid in the development of software.

SVS: Sequoia Voting Systems; manufacturer of several common voting systems.

VVPAT: Voter Verified Paper Audit Trail; a mechanism to generate a paper trail for DRE voting machines.

B Calculations for Population Share

In order to get an estimation of the prevalence of specific voting machines, it was necessary to calculate what we refer to as a *population share*. This population share is intended to represent the fraction of voters whose election process uses a given machine. In this section, we discuss how we calculate this value and the limitations of these calculations.

B.1 Calculations

The calculation of the population share begins with the Verified Voting voting machine database [15]. This data was procured as a JSON object with more information than needed. Specifically, we focused on the keys:

- `opscan`: Boolean indicating whether this system is an optical scanner.
- `bmd`: Boolean indicating whether this system is a BMD.
- `dre`: Boolean indicating whether this system is a DRE.
- `make`: The name of the manufacturer of the device in this entry.
- `model`: The manufacturer-given model name of the device in this entry.
- `name` and `county_name`: These two fields contain varied information about the locality of the device concerned by this entry. In most cases, `county_name` contains the county name and `name` contains the name of the state, however presumably depending on the source dataset, both values might be occupied with a county, or one may be blank.

- `current_reg_voters`: This field counts the current registered voters in the locality specified by `name` and `county_name`.

We repeat the following process three times, once for HFOS/BFOS (`opscan`), once for BMDs (`bmd`), and once for DREs (`dre`).

Using the fields outlined above, we exclude any hybrid system which has more than one of the `opscan`, `bmd`, or `dre` values set. With all non-hybrid machines, we append a tuple with the remaining fields (`make`, `model`, `name`, `county_name`, and `current_reg_voters`) to a list.

Once this process is complete, any duplicates in this list are removed[32], the resultant set has an entry for each unique machine used in any capacity[33] in each precinct or other locality[34].

Using this set of machines, we assemble a dictionary in which the keys are each of the unique machines from the set described above. For each entry in the set, we increase the corresponding dictionary value by the `current_reg_voters` field amount, representing an increase in the total number of voters represented by this specific machine.

Finally, in order to generate a percentage, we calculate the total number of voters represented by all machines in the dictionary. We use this value to calculate a percentage for each machine. It is noteworthy that this percentage (the *population share*) represents the rough fraction of the total population of a machine category (HFOS/BFOS, BMD, DRE) which that machine services.

B.2 Limitations

- This calculation method only includes non-hybrid machines. There are only a couple hybrid machines, therefore these omissions are negligible.

- The population values used do not represent the actual population using a specific voting machine during election, rather the total registered voters in the precinct or locality which makes use of this machine. This limitation is inherent to the dataset, but does not compromise the calculation of rough population share for different machines.

- We include some machines with specific purposes in this count as the dataset provides no method for determining if a machine is used exclusively for these special purposes. Omitting these would remove a significant number of machines used for these special purposes and also used by regular voters. These include machines used for:

  – Accessibility (`in_precinct_accessible`)

  – Early voting (`early_in_person_standard`, `early_in_person_accessible`)

  – Absentee voting (`absentee`, `absentee_accessible`)

[32] Usually duplicates occur as a result of the dataset including multiple election officials or state officials with the same machine information included for each.

[33] For accessibility, standard, early accessibility or early standard voting.

[34] The sources for this dataset vary, therefore some entries have locality entries for their state.