Recount 2016: A Security Audit of the U.S. Presidential Election

Abstract

In this paper we analyze the computer security aspects of the 2016 U.S. election and subsequent recounts in Michigan, Wisconsin, and Pennsylvania. We present a revised election threat model that is much more vulnerable than previously thought, due to centralization and difficulty of invoking defenses against threats. We examine the data generated by the election and recounts, ultimately weakly concluding that election hacking probably did not occur to such an extent as to effect outcomes in Wisconsin and Michigan. We also explore the broader lessons about security in practice that can be drawn from the recount experience, and provide recommendations for easy ways to make the electoral system significantly more robust.

1 Introduction

Donald J. Trump became the 45th President of the United States amid a cloud of concerns. Despite winning the election, Trump has maintained that "millions" of votes were cast illegally [36]. Concurrently, the U.S. government's intelligence agencies issued a stark statement (hereafter, the "ODNI report") [34] about Russian influence on the U.S. election, claiming (emphasis original):

> **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.** We have high confidence in these judgments.
>
> **We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.** All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

While the ODNI's assessments are incendiary, they make an intriguing disclaimer (emphasis original):

> Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. **DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.**
>
> **We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes.**

While the ODNI report makes no statements as to the sources and methods used to reach their assessments, a Russian intent to influence the U.S. election, along with a variety of known security vulnerabilities in existing voting systems (see Section 2), raises serious concerns. We expect this reasoning went into the Department of Homeland Security's designation of election systems as "critical infrastructure" [37].

1.1 Recount efforts

Trump's national victory hung on close races in several states, including Wisconsin, Michigan, and Pennsylvania, where the Green Party's presidential candidate Jill Stein chose to request recounts in an effort to protect the integrity of the election [15].

A number of academic computer security experts filed affidavits in Stein's Wisconsin case[1]. Ultimately, a full

[1] http://www.jill2016.com/wirecountfilings

recount was conducted statewide, although many counties that use optical scan systems chose to recount their ballots through the same optical scanners rather than using hand tallies or suitable audit procedures to rule out any systematic discrepancies in the electronic tallies. (We discuss different voting technologies and their audit properties in Section 2.)

Recounts in Michigan were ultimately halted by a court order, focused narrowly on whether Stein had any standing for requesting the recount [2]. Before its termination, the Michigan recounts did uncover serious concerns in Detroit, where ballot boxes with "too many votes" or broken security seals were not eligible for recounting [22].

Recounts in Pennsylvania never got off the ground [11], with Stein lacking "proof" of malfeasance, despite the whole purpose of the recount being to identify evidence of such malfeasance.

There was a separate recount effort in Nevada, unaffiliated with Jill Stein, instead requested by independent candidate "Rocky" Roque De La Fuente mounted in Nevada. In the nine counties where the recount occurred, the totals changed by only 15 votes, falling below a statutory level that might have triggered an automatic statewide recount [26].

1.2 Research questions

Wisconsin and Michigan votes are largely cast on paper with electronic tallying. Pennsylvania votes are largely cast electronically, with no paper record of any kind. With the data made available in the wake of Stein's recount efforts, we can analyze the reported election data for anomalies. We can also analyze the policies and procedures of these states and offer suggested improvements, such that if the Russians or other skilled cyber threat actors wish to manipulate our elections, we will be more likely to detect and thwart such future actions.

2 Background

TODO: Dan: please revise **TODO:** cite voting machines?

Elections in 2016 in the vast majority of U.S. districts relied on some form of computer to aid in ballot tabulation [42]. This technology can be broken into two categories: direct-recording electronic voting machine (DRE), and hand-marked optical scan tabulation (opscan). We provide a brief overview of each below, as well as a summary of security results for specific instances of each kind of machine.

2.1 Direct-Recording Electronic Voting

DREs have existed in U.S. elections since 1974 [18], and some machines which entered the market in the 1980s are still used today [41].

However, DREs did not have the ubiquity they do now until after the 2000 election and subsequent legal quagmire surrounding outmoded punch card voting technology [28]. Congress passed the Help America Vote Act in 2002, which appropriated more than $3 billion for states and counties to replace their voting technology [40]. Using this money, many counties eagerly purchased the "state-of-the-art" voting technology at the time: touchscreen computers with an intuitive voting interface, support for complicated ballots and disabled voters, and fast tabulation on election night. Votes are stored in internal memory and then transferred to a central tabulator that process input from all the voting machines and output the result of the election, just like in early DRE models. Examples include the Diebold AccuVote TS and TSx, the ES&S iVotronic, or the Hart Intercivic eSlate, and the AVC Advantage and Edge, which can all be seen in Figure 1. At the time of writing, approximately 30% of votes in the U.S. are cast on DREs [42].

TODO: Make this less terrible While these machines were popular with both voters and election officials, it soon became evident that these machines have some severe drawbacks. Lack of an external record of votes means that if the machine produces incorrect results for any reason, it is impossible to fix without running the election again. The machines are prone to error, due to design issues like resistive touch screens that require frequent calibration and software bugs.

2.1.1 Voter-Verified Paper Audit Trails (VVPAT)

In response to a lack of an independent record to help assure the correct result and reconcile any issues upon the completion of the election, the Voter-Verified Paper Audit Trail serves as another, independent record of each voter's vote [29]. Upon casting a vote with a DRE, the voter is also presented with a paper printout of his or her vote, which she can use to confirm that the machine properly registered her selections. Additionally, the paper can aid in post-election audits and recounts as another check on the results produced by the machines.

2.2 Optical Scan Voting

An alternative solution to the lack of evidence produced by DREs is somewhat the inverse of VVPAT: voters fill out a paper ballot and then computers tabulate results by scanning the ballots. Ballots can either be fed into scanners by each voter (precinct-count), or they can be collected in a ballot box and scanned all at once, often in a central location (central-count). Examples of opscan machines include the ES&S Model 100, Optech Insight, and Diebold AccuVote OS, which can be seen in Figure 1.

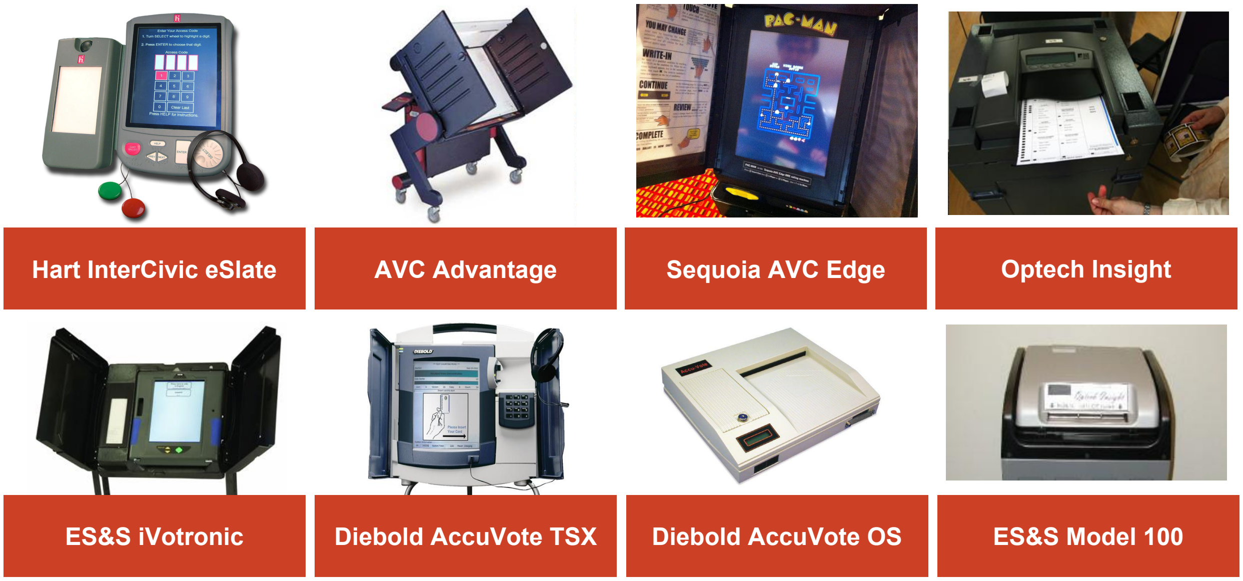

Figure 1: Opscan and DRE machines used in the U.S.

2.3 The insecurity of voting systems

Failures of DREs in practice prompted heavy scrutiny from multiple parties. In 2007, the states of California and Ohio carried out reviews of many of the machines in use at the time [5, 27]. Independent academic studies such as those done by Feldman et al. [14], Kohno et al. [20], Hursti [17], Siefers [35], have all shown that many DREs are woefully insecure and ripe for attack. As DREs without VVPATS lack evidence to verify their results, the are especially attractive targets. As a result of academic security work over the past decade, 70% of votes in the U.S. are cast with some form of paper backup, as seen in Figure 2.

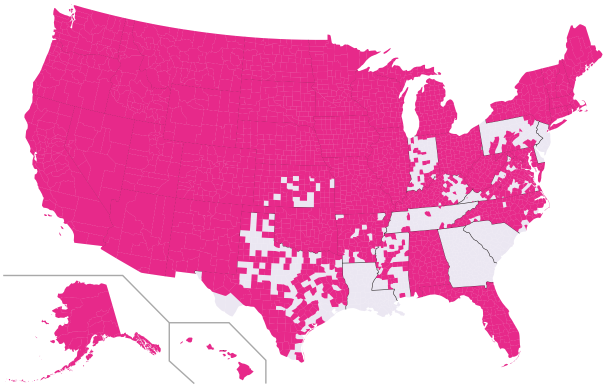

Figure 2: U.S. counties voting with a paper record

However, this is not to say that opscan systems are perfectly secure either. Results like the Hursti hack [16], Aviv et al. [1], the California Top-to-Bottom Review [5], and Ohio EVEREST project [27] have all found significant vulnerabilities in both the hardware and the tabulation software used by these systems.

3 Threat Modeling

Prior voting work has often spent a great deal of time considering the threat model for elections. As we shall see, in light of the events leading up to the 2016 election, many of these models failed to take into account many factors that we discovered throughout our observation and involvement in the election.

3.1 The Old Threat Model

Historically, voting security research has focused on a rather limited set of adversaries and a relatively small attack surface. Election security has largely revolved around providing mechanisms to enable trust in systems that may be tampered by insiders, manufacturers and common criminals. Many cryptographic techniques developed or used for voting attempt to ensure the anonymity of the voter: from the Australian ballot to mixnets [6], to the Benaloh challenge model [3], techniques have focused on preventing coercion or vote buying, and giving voters confidence that their votes count.

Current election security practices generally focus on air-gapping machines [13], relying on the decentralized nature of U.S. elections [4, 21], and (in some cases) providing a paper record to fall back on if needed [25].

3.2 A Better View of the Threat Landscape

TODO: Tighten this up a bit. Maybe put companies in a table (company:states)? As we have already discussed, 2016 provides a significantly different picture for election than previously thought. That there is now evidence of an adversary with nation-state level resources significantly changes the proposition for defense. Moreover, through our exploration of the inner workings of most U.S. elections in practice, we discovered that in many cases the safeguards relied upon by election officials are either non-existent or underutilized.

Elections are not as decentralized as often assumed. Many counties or municipalities rely on third-party business to coordinate and supply election equipment. For instance, in the state of Michigan, Governmental Business Solutions[2] (GBS) and Election Source[3] service 75% of counties. These businesses produce all tamper-evident seals and locks, and also provide much of the equipment needed to maintain voting machines. In some cases, these companies also program the memory cards that are used by voting machines on election day to collect and tabulate votes.

Companies like this are active in many states, and often companies are active in multiple states: GBS in Michigan, Illinois and Indiana; Election Source in Michigan, West Virginia, Missouri, Ohio, and Oklahoma; Command Central[4] in Minnesota and Wisconsin, etc. Any infiltration of a company like this could potentially affect millions of votes across multiple states. , and it is unlikely that they deploy the kind of sophisticated defense needed to fend off a nation-state level adversary. Small businesses like these would stand no chance against an attack akin to Stuxnet [19].

Finally, prior to our intervention, *very* few votes were going to be checked against their paper backups. Many states often have cursory auditing available, wherein a handful of ballots are sampled and checked against their electronic copies, but this is a far cry from risk-limiting audits (RLA) [24], the only way short of a full recount to establish confidence in election results.

3.3 Revised Threat Model

After more fully grasping the threats present in the 2016 election, and in the face of an unexpected result, we set out to build a threat model that we could test against data that would be available to us through the only legal way we could examine election evidence: a recount.[5] Below we discuss three classes of adversary, and what an attack would look like.

3.3.1 Nation-state: cyber

As we have already discussed, it was clear that a nation-state adversary was attempting to disrupt the election, running kompromat campaigns, exfiltrating information from voter databases, and otherwise sewing uncertainty about election results. Would this adversary continue to escalate this campaign and actually attack the mechanism by which Americans cast their votes?

There are significant points of centralization to the election system, and malicious attacks that spread via electronic means are already known [14]. Moreover, given the lack of best cyber security practices.[6] In theory, it is feasible for a nation-state level adversary to carry out an attack without ever setting foot in the U.S.

This attack would likely have an effect in many precincts in a targeted state or set of states, and would be easily discovered by examining the physical record of the vote and comparing with the electronic record. An RLA or recount would report a different outcome in the face of such an attack. This attack would not necessarily affect only one kind of voting machine or voting method.

3.3.2 Insiders: cyberphysical

In this scenario, adversaries are election officials, voting machine vendor employees, and third parties involved in ballot programming and voting machine maintenance. An employee could introduce malware that could spread from machine to machine, potentially affecting all machines serviced by that employee, company, or election district. Additionally, an insider could have access to the physical record of the ballots, and could thus change recorded results in both places.

In this attack, a recount or RLA may not significantly diverge from the original election result, but we would expect a breach of the audit trail in some significant way (broken ballot seals, unaccounted for ballot bags, etc.). The electronic and paper records would disagree, or we would see some sign of tampering on the physical evidence, or both.

3.3.3 Outsiders: physical

This is the least powerful kind of attack, wherein an attacker would have to physically access each machine to compromise it. This could be accomplished by infecting the machine will malware by swapping its memory card with an infected version, physically disabling the machine, or tampering with the physical audit trail. A recount or RLA may not detect this kind of attack, since it would

[2] https://www.gbsvote.com

[3] https://www.electionsource.com

[4] https://ccelections.com

[5] The legalities of recounts will be discussed further in Section 4.

[6] For instance, here's an interview with an election official in Lehigh County, PA discussing data transfer between the ballot programming machine and the voting machines, on commodity USB drive: https://www.youtube.com/watch?v=xbkWg5LbsyM

have a small effect on the overall results that might not be distinguishable from noise, but there would likely be evidence of physical tampering.

3.3.4 Restrictions

These three classes of attack certainly do not cover the total space of threats to elections, but they are the kind of attacks that we were able to look for via a recount. We explicitly exclude things like denial of service, voter suppression, or attackers that go to lengths to preserve the audit trail by replacing seals, forging ballot manifests, and so forth. These attacks are generally visible or require a level of sophistication and care that it would likely be detected by the traditional safeguards already baked into elections.

4 The 2016 U.S. Presidential Election

Up to this point, we have been largely treating elections in the United States as a homogeneous event. In reality, the election landscape is complex, with different methods of voting and legal constraints even within counties. To provide better context, we discuss the three states we attempted to recount here.

4.1 Wisconsin

The state of Wisconsin is perhaps one of the most unique in the nation, in terms of diversity of voting procedure. While in most states counties purchase election equipment and administer elections, in Wisconsin individual municipalities do so [8,42]. As seen in Figure 3, Wisconsin uses opscan technology for the majority of their votes. Roughly 10% of votes in 2016 were counted by hand, and DREs are infrequently used for HAVA accessibility compliance. Nearly 10% of votes in 2016 were cast on voting machines from Command Central. The margin of victory for Donald Trump was 22,748 votes, or 0.7%.

TODO: table for voting equipment? **TODO:** table for election results? **TODO:** deal with WI map not reflecting reporting units **TODO:** Discuss pre-election polling?

4.1.1 Auditing

After each election, Wisconsin randomly selects 100 reporting units (at least 5 using each kind of voting method) and hand recounts all ballots in each reporting unit for four contests, including the top contest and three randomly selected contests [7]. For context, there are 3,635 reporting units in Wisconsin, averaging 819 votes per unit in 2016. On average, just under 2.8% of ballots are counted by hand in the absence of a recount.

Wisconsin law does not allow for any other kind of election audit outside of this one, except for a full recount. Any candidate may request a recount in any number of wards provided he or she can pay the filing fee based on the number of wards to be recounted [10]. Upon filing a recount must be completed by the federally mandated “safe-harbor” deadline of one week before the electoral college votes (in 2016, this was December 12th, the electoral college voted on the 19th). Recounts are conducted by means determined by counties, and the 2016 Wisconsin recount proceeded with 51 counties recounting by hand, 9 by opscan, and 12 using a mix [9].

4.2 Michigan

The state of Michigan mandates that all votes are cast via an opscan ballot [33], and as shown in Figure 3, Michigan only uses three different models of voting machine, and each county only uses one of the three. GBS and Election Source are active in 75% of Michigan counties. In 2016, Donald Trump won the election by 10,704 votes, or 0.3%.

4.2.1 Auditing

Like Wisconsin, the Michigan Bureau of Elections randomly selects reporting units to audit [31]. In 2016 Michigan audited 179 reporting units statewide [30], and an additional 136 units in Detroit and 45 other jurisdictions [32].

Also as in Wisconsin, no other audit may be performed in Michigan except a recount initiated by an “aggrieved” candidate [23]. The Board of Canvassers decides the method of recount, and in 2016 chose to do a full recount by hand [12].

4.3 Pennsylvania

Pennsylvania still allows for the use of DREs without any paper record, and 82% of votes in Pennsylvania were cast in this way in 2016. Pennsylvania also has some of its election equipment maintenance and ballot programming done by ElectionIQ, a company based in Ohio.[7]

Donald Trump won Pennsylvania by 44,292 votes, or 0.7%.

4.3.1 Auditing

Pennsylvania audits at least 2,000 votes in each county, or up to 2% of the total votes cast [38]. However, since most counties use DREs, this audit “recounts” electronic copies of the vote in most cases and does not offer sufficient evidence for confidence in the election outcome.

[7] http://http://electioniq.net/

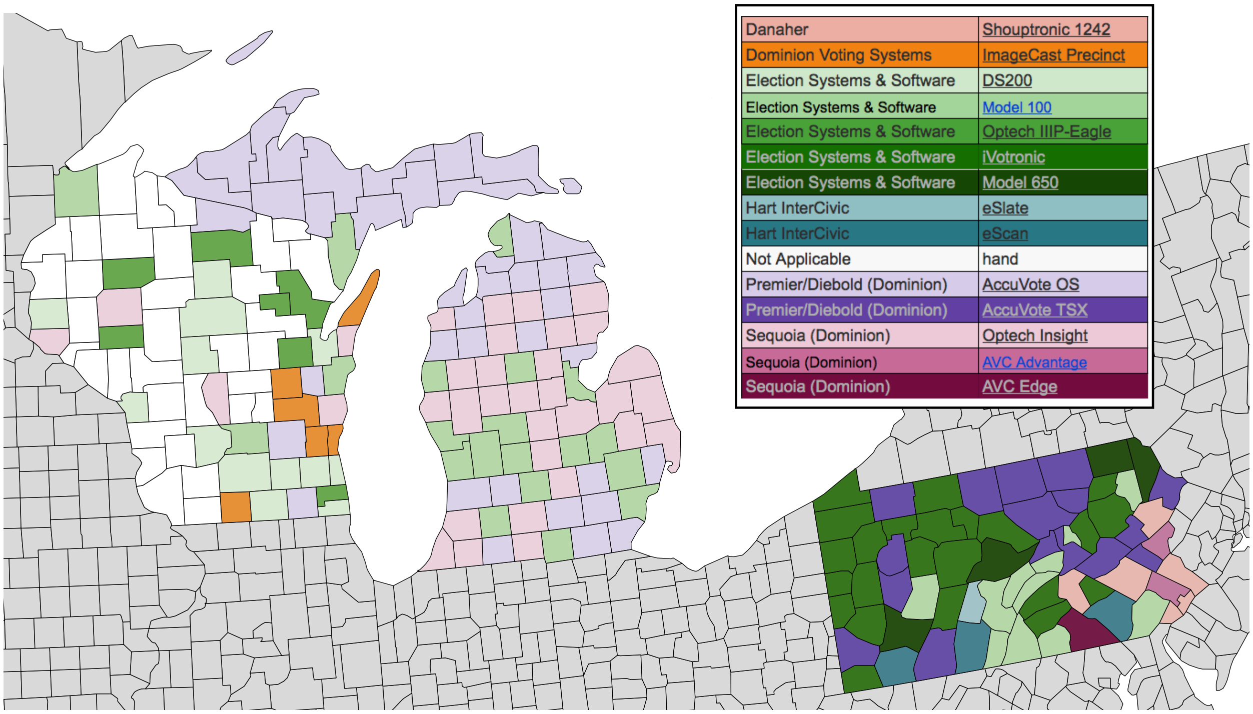
Danaher | Shouptronic 1242
Dominion Voting Systems | ImageCast Precinct
Election Systems & Software | DS200
Election Systems & Software | Model 100
Election Systems & Software | Optech IIIP-Eagle
Election Systems & Software | iVotronic
Election Systems & Software | Model 650
Hart InterCivic | eSlate
Hart InterCivic | eScan
Not Applicable | hand
Premier/Diebold (Dominion) | AccuVote OS
Premier/Diebold (Dominion) | AccuVote TSX
Sequoia (Dominion) | Optech Insight
Sequoia (Dominion) | AVC Advantage
Sequoia (Dominion) | AVC Edge

Figure 3: Wisconsin, Michigan, and Pennsylvania along with equipment in use in each county
TODO: Label states, a better key

Recounts, as in the other two states, are the only means of obtaining an additional audit. In Pennsylvania, recounts are triggered automatically with close margins. Candidates may file petitions to initiate a recount, or three voters in a district may also file to initiate a recount in that district [39].

5 Performing an Uninvited Post-Election Audit

TODO: Alex

6 Analysis

TODO: Walter, add tables, brief discussion **TODO:** Matt provide more discussion, revise

7 Lessons and Recommendations

TODO: Dan, Alex

8 Conclusion

References

[1] Adam Aviv and Pavol Černy and Sandy Clark and Eric Cronin and Gaurav Shah and Micah Sherr and Matt Blaze. Security Evaluation of ES&S Voting Machines and Election Management System. In *Proceedings of the Conference on Electronic Voting Technology*, page 11. USENIX Association, 2008.

[2] Tresa Baldas, Kathleen Gray, and Frank Witsil. *Federal judge's ruling halts Michigan presidential election recount*. Detroit Free Press, December 2016.

[3] Josh Daniel Cohen Benaloh. *Verifiable Secret-ballot Elections*. PhD thesis, Yale, 1987. AAI8809191.

[4] Bump, Philip. Rigging an election is a lot harder than you might think. *Washington Post*, October 2016.

[5] California Secretary of State's Office. Top-to-bottom review of electronic voting systems, 2007. http://wwws.os.ca.gov/elections/voting-systems/oversight/top-bottom-review/.

[6] David Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. *Commun. ACM*, 24(2):84–88, 1981.

[7] Wisconsin Election Commission. 2016 voting system audit requirements. http://elections.wi.gov/sites/default/files/memo/20/2016_audit_procedures_pdf_15417.pdf.

[8] Wisconsin Election Commission. Voting equipment. http://elections.wi.gov/elections-voting/voting-equipment.

[9] Wisconsin Election Commission. County recount cost estimates and counting methods. http://elections.wi.gov/sites/default/files/story/presidential_recount_county_cost_estimate_and_reco_16238.pdf, November 2016.

[10] Wisconsin Election Commission. Election recount procedures. http://elections.wi.gov/sites/default/files/publication/65/recount_manual_11_2016_pdf_17034.pdf, November 2016.

[11] Steve Eder. *Jill Stein's Pennsylvania Recount Effort Is Dealt a Major Setback*. New York Times, December 2016.

[12] Paul Egan. Deadlock: Board vote means michigan presidential recount may proceed. *Detroit Free Press*, December 2016.

[13] Egan, Paul. Michigan elections director doubts vote-hacking in presidential count. *Detroit Free Press*, November 2016.

[14] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, EVT '07, August 2007.

[15] Prachi Gupta. *Jill Stein on What's Next With the Recount Effort in Wisconsin, Michigan, and Pennsylvania*. Cosmopolitan Magazine, December 2016.

[16] Harri Hursti. Critical security issues with Diebold optical scan design. The Black Box Report, July 2005. http://www.blackboxvoting.org/BBVreport.pdf.

[17] Harri Hursti. Critical security issues with Diebold TSx (unredacted), May 2006. http://www.bbvdocs.org/reports/BBVreportIIunredacted.pdf.

[18] Douglas W. Jones and Barbara Simons. *Broken Ballots: Will Your Vote Count?* University of Chicago Press, 2012.

[19] Kim Zetter. An Unprecedented Look at Stuxnet, the WorldâĂŹs First Digital Weapon. *Wired*, November 2014.

[20] Tadayoshi Kohno, Adam Stubblefield, Avi Rubin, and Dan S. Wallach. Analysis of an electronic voting system. In *25th IEEE Symposium on Security and Privacy*, pages 27–42, 2004.

[21] Kopan, Tal. No, the presidential election can't be hacked. *CNN*, October 2016.

[22] Joel Kurth and Jonathan Oosting. *Records: Too many votes in 37% of Detroit's precincts*. Detroit News, December 2016.

[23] Michigan Election Law. 168.862 fraud or mistake in canvass or returns of votes; recount petition by candidate. http://www.legislature.mi.gov/(S(ncpznawnheyygbjptsh5kqod))/mileg.aspx?page=getObject&objectName=mcl-168-862.

[24] M. Lindeman and P. B. Stark. A gentle introduction to risk-limiting audits. *IEEE Security and Privacy*, 10:42–49, 2012.

[25] Livengood, Chad. Mich.'s elections designer: No 'easy path to fraud'. *The Detroit News*, October 2016.

[26] Jessica McBride. *Nevada Recount Results: Final Tallies Show Only 15 Vote Change*. Heavy, December 2016.

[27] Patrick McDaniel et al. EVEREST: Evaluation and validation of election-related equipment, standards and testing. http://www.patrickmcdaniel.org/pubs/everest.pdf, December 2007.

[28] Mebane, Walter R. The wrong man is president! Overvotes in the 2000 presidential election in Florida. *Perspectives on Politics*, 2(03):525–535, 2004.

[29] R. Mercuri. A better ballot box? *IEEE Spectrum Online*, October 2002.

[30] Michigan Bureau of Elections. Jurisdiction/precinct list: Post-election audits. http://www.michigan.gov/documents/sos/Post_Election_Audit_List_449745_7.pdf.

[31] Michigan Bureau of Elections. Post-election audit manual. http://www.michigan.gov/documents/sos/Post_Election_Audit_Manual_418482_7.pdf.

[32] Michigan Department of State. Executive summary of audits conducted in detroit and statewide in relation to the november 8, 2016 general election. http://www.michigan.gov/documents/sos/Combined_Detroit_Audit_Exec_summary_551188_7.pdf.

[33] Michigan Secretary of State. Voting equipment. http://www.michigan.gov/sos/0,4670,7-127-1633_8716_45458---,00.html.

[34] Office of the Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent US Elections*, January 2017.

[35] Joseph Seifers. Analysis of a Danaher / Shouptronic 1242 Electronic Voting Machine. http://perfect.cse.lehigh.edu/Documents/JoeSiefersReportSpring2008.pdf, 2008.

[36] Michael D. Shear and Emmarie Huetteman. *Trump Repeats Lie About Popular Vote in Meeting With Lawmakers*. New York Times, January 2017.

[37] Tim Starks. *DHS labels elections as 'critical infrastructure'*. Politico, January 2017.

[38] Purdon's Pennsylvania Statutes and Consolidated Statutes. 3031.17. statistical sample. https://govt.westlaw.com/pac/Document/NE8D7C3E0343011DA8A989F4EECDB8638.

[39] Purdon's Pennsylvania Statutes and Consolidated Statutes. 3154. computation of returns by county board; certification; issuance of certificates of election. https://govt.westlaw.com/pac/Document/NEB3CDD00343011DA8A989F4EECDB8638?

[40] United States House of Representatives, 107th Congress. Help America Vote Act of 2002, January 2002. https://www.eac.gov/assets/1/workflow_staging/Page/41.PDF.

[41] Verified Voting Foundation Inc. Danaher Shouptronic 1242, 2016.

[42] Verified Voting Foundation Inc. The Verified Voting Foundation Verifier, 2016.