Hacking the White House: Election Fraud in the Digital Age

A thesis presented by

Brian Kyle Plancher

To the Department of Computer Science

In partial fulfillment of the requirements

For the degree of Bachelor of Arts with honors

Harvard College

Cambridge, Massachusetts

March 29, 2013

"The elective franchise, if guarded as the ark of our safety, will peaceably dissipate all combinations to subvert a Constitution, dictated by the wisdom, and resting on the will of the people."

–Thomas Jefferson (Foley 1900, 842)

"There is probably no other phase of public administration in the United States which is so badly managed as the conduct of elections. Every investigation or election contest brings to light glaring irregularities, errors, misconduct on the part of precinct officers, disregard of election laws and instructions, slipshod practices, and downright frauds."

– Joseph P. Harris, Brookings Institute 1930 (Gumbel 2005, xiv)

Abstract

Our founding fathers fought a war to remove the shackles of colonial tyranny and install a democracy guided by the principle of “one man one vote.” The modern American electorate, however, is losing confidence in the integrity of its voting system. At the same time, computer security researchers have revealed that many of today’s voting machines are highly flawed and vulnerable to cyber-attack. Together this begs the question: are American elections safe from attack? This thesis is an exploration of not only how credible the threat of a stolen election is given the voting systems operating today, but also in what ways a theoretical attack might take place and what protective measures can be implemented to prevent an attack. This thesis first examines why these vulnerabilities exist by exploring the history of voting machines and revealing that the persistence of these flaws is caused by repeated shifts in the relative importance of privacy, usability, transparency and cost. It then explores what types of attacks can occur by focusing on both attacks against the system in which the machines operate, and those against the machines themselves. This reveals that scalability, ease of access, and likelihood of detection determine the profitability of each attack. Where, when and how an attack against the voting system will occur is explored next by simulating a theoretical attack against the 2012 election. Finally, this thesis ends with a discussion of how to safeguard the American electoral system. This thesis concludes that: paper trails and audits are effective measures to radically increase the difficulty of attack, future systems need to be designed to balance privacy, usability, transparency and cost, voter education is a vital part of any security strategy, and safeguards against insider influence on the voting process can greatly hinder the scalability of an attack. Elections can be made quite secure if these conclusions are considered, followed and implemented.

Before I begin I have to thank the people that made this thesis a possibility: my advisor Professor Greg Morrisett who not only came up with the original idea for the thesis but also helped guide me through the process, my readers Professors Stephen Chong and David C. Parkes and also Victor Shnayder who all helped me get this thesis off the ground, and Annie Knickman for her huge help with editing. I also have to thank my mother, Jill Plancher, who as usual was always there for me with guidance, support and editing. I probably wouldn't have made it through college without her paper advice. Finally, I have to thank the rest of my family and friends for supporting me through this process.

Table of Contents

Table of Figures

Introduction

Arrow's impossibility theorem states, "Any constitution that respects transitivity, independence of irrelevant alternatives, and unanimity is a dictatorship (Geanakopolos 2005)." In other words; no democratic voting system can be perfect. With the Electoral College system in place and the entrenchment of the Democratic and Republican parties in certain states, the United States electoral system is anything but free from this conclusion. At the same time, reports have recently surfaced that reveal cases of voter fraud in the United States, and demonstrate that flaws in the voting machines make them vulnerable to attack. This raises the question: could someone actually steal an American election today? To fully answer this question one must explore not only the voter registration system, the absentee balloting system, the design of the voting machines and the manufacturing of the voting machines, but also the training of poll workers, the design of ballots and all of the other small parts of the modern voting system. Since many of these topics alone could consume an entire dissertation, I decided to focus on providing a high level synthesis of all of these topics in order to determine how dangerous each of the flaws are in broader context, and to determine whether someone could covertly steal the presidential election in the United States.

I chose to focus on the presidential election in order to assume away many of the idiosyncrasies of the many different voting districts across the nation and instead focus on the larger issues at play. For the same reason I often compress many different models of voting machines into broader classes and throughout the paper I consider only the standard polling place equipment as the accessible polling place equipment would be used by only the less than one half of a percent of Americans who are legally blind (Associated Press 2009). I also decided that the goal of the attack was to covertly steal the election because this is the type of attack that could secretly change the course of human history given the power placed in the President's hands. Furthermore, as the recent revelation of the cyber-attack on Miami-Dade County's absentee balloting system demonstrates (Fineout 2013), this nation has only seen the beginning of cyber-attacks on its voting systems. However, in order to fully understand the security of the current system, I make note of some attacks that crossed my mind or turned up in my research that while harmless to (or impossible to pull off for) a national election, could have a huge impact on a smaller more localized election, or could have a large impact nationally but would be quite risky.

In order to understand why the current system has developed with so many flaws, Chapters 1 and 2 focus on the historic development of the modern voting systems and reveal that repeated and rapid shifts in priorities among privacy, usability, transparency and cost have led to the development of the flawed voting systems. Chapters 3, 4 and 5 focus on the specific types of attacks that can be perpetrated against the modern voting systems and find that both attacks against the machines themselves and the larger system in which they operate have varying degrees of scalability, risk, and potential reward. Chapter 6 then lays out my theoretical attack against the 2012 election showing that flaws in a few key districts can impact the outcome of a national election. Chapter 7 builds off of the analysis presented in the earlier chapters to recommend improvements to the voting systems in both the short and long run. Recommendations focus on effective voter education, paper trails, and audits and call for future systems that are developed with a balance between privacy, usability, transparency and cost.

Chapter 1: A Brief History of Voting In America

"When it comes to election malfeasance, the two parties are separated not so much by morality or democratic scruples as they are by straightforward, naked access to power and the opportunity it affords one of them (Gumbel 2005, 224)."

The American electoral system is considered by many to be a prime example of best practices for a successful democracy. Elections are assumed to ensure efficiency and privacy while still providing transparency and upholding the principle of one man, one vote. Unfortunately, that is simply not the case, and recent elections paired with emerging news sources such as Twitter (Kwak, et al. 2010) have begun to bring this unfortunate fact to light. From long lines at the polls, malfunctioning and poorly calibrated machines (Jauregui 2012), to accusations of outright fraud (Stiner 2012), the United States electoral system is not where it needs to be. In fact, in reference to the 2012 election, the Washington Post even stated, "To many observers, it seemed ludicrous that a country as advanced and as wealthy as the United States can't figure out how to hold a decent election (Plummer, Five ways to make long elections lines shorter 2012)." And, despite various news sources proposing solutions, none of them seem to agree on the most important problem with the current system. The Smithsonian is pushing for an overhaul of the voter registration system (Gambino 2012), while the New York Times blames issues on poorly trained poll workers and confusing new machines (Taylor 2012), while the Washington Post suggests more early voting will solve many problems (Plummer, Five ways to make long elections lines shorter 2012). Clearly there is a lot to fix and a lot to be done. In order to understand why the errors in the current systems developed and how these errors can be prevented in the future, one must analyze the history and development of the current voting systems because as President Harry S. Truman stated, "The only thing new in the world is the history you don't know (Howington 2013)."

A tour through the history of the American electoral process reveals cyclic flaws and points towards clear opportunities and motivation for someone to exploit the new electronic voting machines to swing an election. These opportunities can be predicted based on four key forces: privacy, cost, transparency and usability as shown below in Figure 1. Over time, the importance of these forces has shifted, often in overly drastic ways, to address immediate issues without regard for potential side effects of those changes. This chapter follows these shifts in early American voting systems and highlights key patterns and weaknesses that provide a backdrop for the next chapter's analysis of the development of modern voting systems. The historical exploration begins at the inception of American democracy, the Constitution of the United States of America.

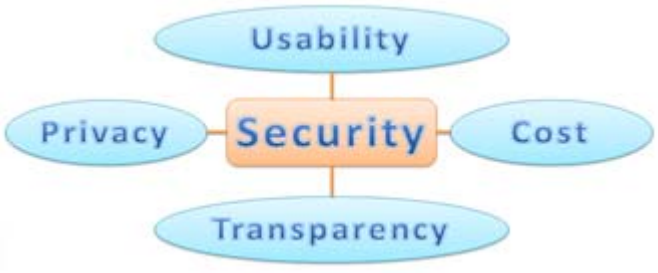

Figure 1: The Security Paradigm

Section 1.1: The Constitution and the Right to Vote

"The Constitution was essentially an economic document based upon the concept that the fundamental private rights of property are anterior to government and morally beyond the reach of the popular majorities (Beard 2002)."

While many features of the Constitution can be exalted as proponents of Democracy, the electoral system is not one of them. In fact, many of the problems the electoral system has faced throughout history can be traced back to the poor design of the system in the Constitution itself. Surprisingly, the right to vote is not guaranteed in any section of the Constitution, or in the Bill of Rights. This major oversight has been abused by political parties to subvert the electoral process in order to claim, reclaim, or maintain power. Paired with the winner-take-all approach of American style elections, as opposed to the proportional style found in Parliamentary systems, the Electoral College makes many votes useless. Only votes in the key "swing states," those states whose electoral votes can go to either party and will swing the election, matter. In fact, the New York Times reported that in the 2008 election, "the presidency could be won with just 22 percent of the electorate's support, only 16 percent of the entire population's (Cowan, Doyle and Heffron, How Much Is Your Vote Worth? 2008)." These distorted rules mean that in close elections, a swing of one percent of the vote in a key state could result in a huge shift of power in American politics for four or more years. The failures in the constitution designed a system that raised the stakes to the point where politicians would do nearly anything to wring out the last couple of votes in swing states and especially in those states' key districts and those districts' key precincts. It therefore comes as no surprise that spending on elections has ballooned to over $1.5 billion for the 2012 presidential election (Ashkenas, Ericson, et al., The 2012 Money Race: Compare the Candidates 2012).With these basic facts in mind it is time to explore the early voting technologies used in the United States.

Section 1.2: 18th and Early 19th Century Voting

"Force and fraud are in war the two cardinal virtues (Hobbes 2003)."

The initial electoral system in the United States was a voice vote in town halls. This was designed to be fully transparent in order to move radically away from the colonial dictatorship that was just defeated in the Revolutionary War. This system led to high moral amongst voters but had the unfortunate side effect of absolutely no privacy. Furthermore, with a growing population this quickly became an unusable system and as such the nation quickly moved to a paper voting system. In the initial paper voting system political parties were responsible for printing their own ballots which resulted in each party printing their ballots on different colors, shapes, and sizes of paper. This had two very positive side effects. For one, voters knew that they were voting for their candidate because the ballot's distinctive nature ensured them of that fact. Secondly, party observers could count the number of votes as the vote progressed and could themselves be a check on the official tally. Thus elections were quite usable and relatively transparent.

Unfortunately, this system also had the side effect of allowing armed gangs to stand guard at polling places and intimidate, coerce or purchase votes to ensure that voters "voted correctly" as shown in Figure 2. Convicted felons who swore to support their local dominant political machine often seemed to "slip through the cracks" of the judicial system (Gumbel 2005, 73-74,113). Ballot stuffing was also a

common occurrence. In South Carolina in 1878, "The Democrats had a tissue-paper ticket of pale-blue color. There were two sizes of this tissue-paper ticket, so that the smaller could be folded in the larger one, and an outsider could not tell that there was more than one ticket being voted (Evans 1917, 7)." Fraud was commonplace, clearly visible and repulsive, so much so that historian Eldon Cobb Evans theorized that, "It is hard [to] imagine a system more open to corruption (Evans 1917, 11)." Nevertheless it continued for the majority of the century until a new system came out that promised a solution to the fraud and corruption through ensuring privacy for voters.

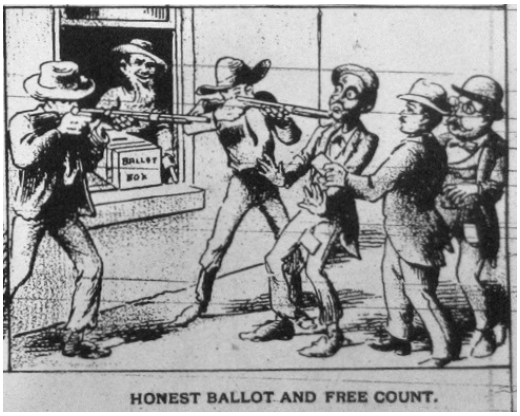

Figure 2: Honest Ballot and Free Count
(Voter Intimidation 1892)

Section 1.3: The Secret Ballot

"In voting, you cannot trust any other party, [y]ou have to be able to be confident that everyone's voice has been heard (Morrell 2012)."

The new system was the secret ballot and while it solved the obvious corruption and ensured privacy in voting, it failed to remove all forms of intimidation and introduced new forms of corruption. These unintended consequences came due to the radical shift in the four forces as privacy was greatly increased at the expense of a large reduction in transparency and usability.

Created and first adopted in Australia in the mid-1800s to curb the riotous nature of elections in the former penal colony (Evans 1917, 17), the secret ballot created a system in which voters were able to select their preferred candidates in private on a single ballot printed by the state. Although first introduced in the United States in Kentucky in 1883, it was not until the 1890 Yates-Saxon Bill in the New York Legislature that the spread of the secret ballot permeated mainstream American politics (Evans 1917, 19-20). Despite its late introduction into the United States it quickly became the default voting system across the nation as it eradicated the obvious fraud in the previous system through its use of private voting areas.

However, the secret ballot was not without its faults and criticisms were quickly launched. Critics first attacked the idea that only printed official party candidates were included on the ballot. Governor Hill of New York originally vetoed the bill stating, "I am unalterably opposed to any system of elections which will prevent the people from putting candidates in nomination at any time" (Evans 1917, 24). Soon after

the ballot design was amended to allow for a write in candidate.[1] However, other issues were not as easily solved.

The first major issue was that power over the election was placed solely in the hands of the election officials. While this is rational at a high level, this major reduction in transparency had unintended consequences that created new ripe areas for fraud. The New York Herald cried out on May 14, 1889, that the new system gave election officials, "an absolute control over the result of any and every election, for only such ballots as these clerks [election officials] chose to deliver to voters can be cast or counted (Evans 1917, 26)." The distribution of fraudulent ballots proved to be less of a long term issue as they were mass produced by states. That said, even before the introduction of the secret ballot, Boss Tweed of Tammany Hall was quoted as saying, "The ballots made no result, the counters made the result (Gumbel 2005, 87)." With the secret ballot in place, this problem was magnified as party officials couldn't make a rough estimate of the number of votes as the vote proceeded, thus there was no outside source able to validate the count. The money for fraud simply got redirected from small payouts to individual voters to massive bribes given to election officials.

To carry out this fraud new tactics were developed by election officials to invalidate votes without changing the official result counting process. The most popular of these was the use of the "short pencil." In this attack, poll workers would stick a pencil lead under their thumbnail and use it to double mark elections, invalidating votes intended for the other party (Gumbel 2005, 117). Further exploitations of the system included "chain voting" which begins with a corrupt pole worker giving a blank ballot to a local party boss. Then, "the local boss would fill it out and hand it to a voter. The voter would then drop the completed ballot in the box and bring the one he was given inside the polling station out untouched for the boss to fill out again and give to the next voter in line (Gumbel 2005, 117)." This attack would thus subvert the entire point of the secret ballot. Finally, election officials could still simply change the final tally numbers.

The secret ballot also led to a huge reduction in usability leading to the unintended consequence of mass voter disenfranchisement. In 1890 in the South over sixty percent of African Americans were illiterate (Margo 1990, 7), and many poor whites and other immigrants were illiterate as well. With the party ballot system in place, the illiterate were able to rely on the party symbols, colors and shapes of the ballots to ensure that they voted for the correct candidates. Now, with a ballot printed in black and white and with only the names of the candidates on the ballot, many of the illiterate or handicapped could not vote (Gumbel 2005, 115). As such, many African Americans, other minorities and poor whites were disenfranchised.

Overall, the adoption of the secret ballot was quite effective at curbing the main type of fraud which it was designed to combat, however it also led to unintended consequences that negatively affected its usage in practice despite the best intentions in its design.

[1] This importance of election systems providing the ability for write in candidates continues today and has a large impact on potential future voting systems and technologies.

Section 1.4: The Lever Voting Machine

"Technology alone does not eliminate the possibility of corruption and incompetence in elections; it merely changes the platform on which they may occur." – Rebecca Mercuri (Gumbel 2005, 173)

The trend of critical unintended consequences greatly affecting voting systems in practice continues with the next system invented, the lever voting machine shown below in Figure 3. This new machine was the first in a line of technological solutions that attempted the fix the American electoral process and is the ancestor of today's voting machines. These machines were first produced around the turn of the 20th century and became commonplace in the mid-1920s (Lee 2009).[2] These machines were designed to mitigate the power placed in the hands of election officials by the secret ballot and to make the process easier and faster for both election officials and voters. However, in the single minded effort to fix a specific transparency problem, the resulting final product actually significantly decreased overall transparency in the voting process.

Figure 3: The Lever Voting Machine
(Everett, The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection 2007)

Lever voting machines were appealing for a variety of reasons. Lever machines counted votes by having a voter flick a bunch of switches to choose candidates and then pull the giant lever to register the vote. Since it was a purely mechanical system, chain voting, ballot stuffing, and short pencil based attacks were impossible. Furthermore, versions of the machine opened their privacy curtain after the lever was pulled notifying the poll workers that the vote was over and preventing voters from double voting. Furthermore, safeguards in the gear system itself could be put in place to prevent over-votes (situations in which a voter choses too many candidates for a position and therefore invalidate their vote for that race). All of these improvements directly made the voting process less fraudulent and less prone to errors. In addition each machine tallied up its own votes which made the tallying process easier and

[2] This is especially impressive given that the lever machines were only decommissioned in New York City in time for the 2010 elections (Chen 2010), although no new machines had been produced since 1982 (Streb 2008, 81).

more efficient for poll workers and saved the state money. In light of all of these facts it is not surprising that they were used in so many states for such a long time.

However, the lever machines were not without their flaws. For one, the election system still necessitated that election officials both record and sum the counts from each machine manually. Election officials could thus still manipulate the results by shaving off a few votes or switching a few votes here or there in order to aid their candidate. Also, write in candidates now had to get their votes counted via a separate process as the lever machines could not handle such votes. With the dominance of the major parties throughout the 20th and 21st centuries, this was fortunately never a huge issue in practice (at least for large national elections) although it was definitely a large design error given the American system's propensity for write in candidates.

The most glaring issue with the lever machines was the lack of any auditable paper record which gutted the transparency of the system. Under earlier paper voting systems, all of the pieces of paper could be recounted if requested. With the lever machines all that could be reviewed was the configuration of the dials on the machines. There was no proof that those numbers corresponded to the votes cast by the voters beyond the guarantees made by the manufacturer. As Andrew Gumbel stated, "[the lever machines] were flawless only if you chose to believe they were; in the absence of physical ballots to go back and check, there was no way to be sure. If one or more of the internal counters malfunctioned, who was to know (Gumbel 2005, 183)?" All a voter could know was that they pulled the lever with the correct switches in place. Beyond that the rest was magically taken care of by the machine. This lack of auditability in this and other voting systems has worried voters for years and spawned an entire research project by Colombia University's Brennan Center for Justine that resulted in the paper "Post-Election Audits: Restoring Trust in Elections." The paper recommends that only in electoral systems in which an audit is possible and the audit is preformed, can the public have any trust in the outcome. Lever machines fail in this regard as any audit of individual votes is impossible and corrupt poll workers who report false results could adjust the machines accordingly.

The final more subtle issue with the lever machines was the systems reliance on the machine manufacturers. This meant that the trusted base was expanded beyond the election officials and poll workers to the employees of the manufacturers of the machines. And, unlike election officials, there were no elections, or pairing of one from each major party, to keep the machine manufacturers employees in check. Making matters worse, most election officials were not mechanical engineers, and as such were not only fully reliant on the device manufacturers for assistance on how to properly configure the machines, but also could not properly audit the machines to make sure that they were working as promised. If the device manufacturers had political leanings or were properly bribed, they could potentially misconfigure their devices to sway an election. Potential evidence of such an event occurred in the 1996 Senate race in Nebraska. In this race between "Chuck Hagel and Ben Nelson, the polls were even days before the election. Yet Hagel won by 15 percent of the vote -- votes counted by a company Hagel had once chaired (A. Cohen 2012)." More recently, the Romney family was reported to have an ownership stake in one of the big election machine manufacturers (Ungar 2012). When moving to a fully technological solution one must be careful to make sure that all of the new players in the system have their incentives aligned correctly. Any misalignment, whether for profit or personal

preference, can lead to disastrous results. If the company cares more about one candidate winning then its future proceeds from supporting multiple future elections, then there is nothing incentivizing the company not to cheat. This great reduction in transparency and lack of auditability worried many and therefore new systems were proposed to solve these issues, and most did so through the use of paper trails. From an attackers point of view this historic vacillation shown by the transition to and, as we will see in the next section, from paper trails is an important point to consider moving forward as systems with paper trails have very different security properties and flaws than systems that do not possess a paper trail.

Section 1.5: Punch Card Voting

"In this manner we have a mechanical check for the tickets, while the ticket is also a check on the register." – J.A. Gray 1899 (Jones, Technologists as Political Reformers: Lessons from the Early History of Voting Machines 2006, 8)

In the 1960s Martin Coyle and University of California Political Science Professor Joseph P. Harris came up with punch card voting systems. While Coyle's company would flounder, Harris's would lead to the creation of the Votomatic, shown below in Figure 4. The punch card systems had many advantages and were designed by Harris in particular to counteract the issues of auditability with the lever machines. However, their unintended reduction of usability led to the 2000 election debacle in Florida (Alvarez and Hall, Electronic Elections 2008, 6).

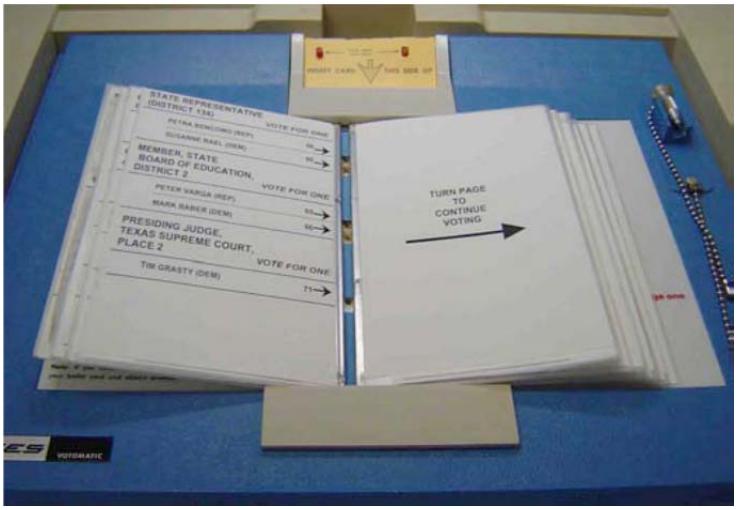

Figure 4: The Punch Card Voting Machine
(Everett, The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection 2007)

This system worked by having voters punch out holes in pre-printed punch cards to indicate their choices. At the end of the day, the cards were counted using a computer system to quickly and accurately tabulate the totals. This new system was therefore advertised as more useable for voters and election officials, and importantly, cheaper than purchasing a similar number of lever machines. By using standard IBM computer punch cards of the day, Harris was able to make the system cheap with one main counter for the district and simple commodity punch cards for the ballots. Furthermore, with no moving or complex parts, the voting booths themselves were very simple with just a few parts designed

to hold the ballot and enable a voter to punch out the correct holes in the ballot. This cheap design also allowed for greatly increased speed in voting by allowing more polling stations per precinct which in turn made it easier for people to vote. Furthermore, IBM bought Harris's company and offered to produce the high-speed vote counters (Votomatic Vote Recorder 2004, IBM n.d.). With the IBM name came immediate trust and comfort from both the American public and the election officials. The ballots also had a write in box and thus made the write in candidate process much more straight forward and simple. This system also still provided users with privacy as the punch cards contained only the vote and no identification data on who the voter was that punched the holes. At first glance, this system greatly improved the overall performance of the voting process for both the voters and election officials.

Most importantly, the system offered a paper trail, solving the transparency issues faced by the lever machines. The punch cards could be hand counted to audit of the counts recorded by the high speed counting machines. In this way regardless of whether or a not the computerized counters were compromised, one could always look back at the punch cards themselves and find the vote totals. This return toward the era of paper secret ballots was one of the largest impetuses for the adoption of the machines. The election process had now sifted from one of black box voting to one of transparent speed counting of hand-countable ballots. The Votomatic got this right.

However, very quickly problems began to surface with the machines. First off, IBM bailed on the small profit margins and high risk for public outcry and licensed the product to various companies (Trombley 1989). As Andrew Gumbel noted, "Few big-name companies have ever shown much interest [in voting machine technology], and of those that have, none has stuck around for long (Gumbel 2005, 188)." With the exit of IBM came the entrance of various small firms who arguably did not have the technical expertise of IBM, and ones that could again potentially be linked to special interests. That is not to say that IBM would have been immune from such a threat, but given the size of the company and the small portion of it that would be dedicated to voting machines it is less likely that the company would intentionally threaten its well-being by producing fraudulent devices to swing one election.

That said, the biggest problems with the machines came from unintended consequences of the new design. The first was the removal of over-vote protection which greatly reduced the usability of the system. Voters could now again accidentally vote twice in an election and would then invalidate their ballot. Similarly to the original attacks on the secret ballot, election officials could effectively "short pencil" the ballot by punching out another hole which would again invalidate the ballot. In a related attack, an election official could vote in a race that the voter did not vote on at all by adding votes to his or her favorite candidate by punching out the given hole in the card (Arnold 1999, 32).

Making matters worse, the ballots were generally designed quite poorly further decreasing usability. This made it difficult for voters to determine which whole in the card should be punched out to vote for each candidate. This confusion made it difficult for the elderly to vote[3] and many of the elderly had trouble punching out the entire hole or the correct hole. These halve punched out holes, or "hanging chads," voided thousands of ballots and spoiled thousands of votes. It is important to note though that

[3] While the illiterate population also struggled, the literacy rate in the United States had reached 90% (Margo 1990, 7). Thus the elderly were the new population that could be abused by ballot design.

the hanging chads were not just the Votomatic's problem, but also a fault of the election officials. Bob Varni founder of C.E.S. the company who bought the rights to the Votomatic explained it this way, "We used to recommend counties buy new [templates for the machines] every six to eight years. If they'd done that in Florida, it would never have got to hanging chads. For lack of a three-dollar part, they blew this whole thing" (Gumbel 2005, 198). Therefore, even with the systems low cost, districts did not have or chose not to spend more money to keep the system in pristine shape. Either way, research shows that this system was the most likely to miss votes (Streb 2008, 83), and ultimately this lack of usability led to the 2000 election debacle and the system's demise.

Section 1.6: The 2000 Election and the Help America Vote Act (HAVA)

"I had hoped to be back here this week under different circumstances, running for re-election. But you know the old saying -- You win some, you lose some. And then there's that little-known third category." – Al Gore, 2004 Democratic National Convention (Gore 2004)

The 2000 election between George W. Bush and Al Gore was a watershed moment for voting technology in the United States due to the notorious failures of the punch card voting system in Florida. Terrible ballot design mixed with old Votomatic machines lead to thousands of accidental incorrect votes. One of the most infamous and obvious failures came out of Palm Beach County where there were a surprisingly large amount of votes for the ultra-conservative Pat Buchanan (given the dominance of elderly Jewish constituents in the county, the selection of an extreme anti-Israeli candidate seemed unlikely). After careful study it was determined that, in the words of Andrew Gumbel:

"[Palm Beach County residents] undoing was the soon-to-be-infamous butterfly ballot layout…The butterfly ballot had caused problems everywhere it had previously been used, but was nevertheless favored by Palm Beach County's miserably incapable election supervisor, Theresa LePore, who thought the county's disproportionately elderly voting population would like the larger type made possible by spreading the presidential ballot over two pages…A political scientist from Berkley subsequently calculated that at least 2,000 [votes] must have been meant for Gore (Gumbel 2005, 206)."

This would have swung the overall election in Gore's favor and therefore the poor usability of the Votomatic paired with the butterfly ballot layout directed changed an entire election.

In the wake of this election, many bills were put in front of congress to federally fund a program to upgrade the voting machines across the country. In 2002, after bitter fighting between special interest groups, the bill was passed. HAVA allocated $3.8 billion dollars in federal funding for the purchase of new voting machine, allowing all of the cash strapped counties in the United States to upgrade their voting systems (G. M. Miller 2004, 3). Despite comments such as "You don't want to be on the bleeding edge with critical systems" by Baltimore County's information technology chief, Tom Iler (Gumbel 2005, 234), most election officials opted for the newest latest and greatest machines because, "Who, after all, could continue to accuse [election officials] of neglect when they were opting for the most expensive, most technologically advanced system on the market? (Gumbel 2005, 229)." At the same time, HAVA included some new stipulations that required better solutions for the handicapped, especially the blind, to allow them to vote easier and in privacy; something paper, punch card or lever based voting never could promise. While new systems emerged to solve many of these issues, the new systems designers neglected to look to the past and repeated failures of the earlier systems explored in this chapter.

Chapter 2: A History of the Modern Voting System

"Ready, fire, aim!"

Due to HAVA the modern voting systems were born in a gold rush. Election officials did not take the time to review the historical record, or the machines themselves, and therefore they chose faulty systems that quickly needed to be upgraded or were quickly proven to be insecure. While President Bush stated at the HAVA signing, "The legislation I sign today will add to the nation's confidence [in the electoral system] (Claassen, et al. 2012, 2)," it actually produced the opposite effect amongst the informed, especially within the computer security community. With election administrators quickly shifting the balance of cost, usability, privacy and transparency without regard to potential side effects, history repeated itself and similar problems seen in the past plagued the modern machines. For a potential attacker this lack of foresight was like Christmas coming early.

Section 2.1: The Direct Recording Electric (DRE)

"[Chief Enginer Robert] Boram was refreshingly honest all around when it came to the realities of computer voting. He told *New York Newsday* in 1992 exactly why it was a mistake to rely on the internal audit mechanism of a DRE as opposed to an independently verifiable paper trail. 'I could write a routine inside the system that not only changes the election outcome,' he said, 'but also changes the images to conform to it (Gumbel 2005, 197).'"

The DRE developed directly from the lever machine and was its natural descendant. In fact, early versions, called full-face DREs, operated exactly like a lever machine. With these machines a voter simply pressed buttons behind candidates' names and pushed a final button instead of flicking switches by candidate's names and pulling a final lever to vote. These early versions came out in the late 1980s but proved to be very unpopular at first as they were more complex and provided few benefits over their lever machine counterparts. In fact, just like lever machines, the layout of the ballot had to be specified before the election and could only be configured in a few different ways. However, just before the 2000 debacle, the next generation of DREs was developed paving the way for the popularity of the devices and the modern machines seen today. These so called dial DREs operated by having a voter vote on one screen for usually one race at a time and move through each race until every race was completed by using a dial to maneuver around the computer screen readout. This provided flexibility in the design of different kinds of voting rules and number of races as each race was processed independently. After voting on the last race a review screen would be shown and then the voter would have the choice to submit or go back and edit races before his or her final submission of the ballot as shown in Figure 5 on the left. While both of these inventions were critical to the development of computer based voting it was the touchscreen DRE that really changed the voting technology game.

Since almost all security researchers refer to touchscreen DREs as DREs and since the dial DRE operates identically to the touchscreen DRE (besides the use of the dial instead of the touchscreen to navigate the ballot), I will be referring to touchscreen DREs as DREs throughout the balance of this paper and if I mean otherwise, I will specify. I also leave it to readers to extend the touchscreen DRE's more detailed explanation in the rest of the section to the dial DRE as they are so similar, and to realize that full-face DREs work and have the same properties as a lever voting machine previously mentioned except that

the vote totals are stored electronically on the machine.[4] Therefore moving forward, most advantages and disadvantages of DREs will also remain true for dial DREs, but those that make use of the screen for presentation will not apply to full-face DREs due to their lack of a programmable screen.

Figure 5: The DRE Voting Machine
(Verified Voting Foundation 2012)

The DRE is essentially at its core, an ATM for voting[5] as shown in Figure 5 on the right. The DRE works in a couple of steps. First, on a centralized Election Management System (EMS), election officials prepare the ballot definition file and export it to some sort of portable media which is then inserted into the machines on Election Day. Voters use the touch screen to select candidates and review their selections and then submit the ballot which is stored electronically on the machine. After the election, the electronic totals are exported to removable media and summed up on the EMS. These machines are especially good at preventing over-votes and under-votes (situations where elections are skipped on a ballot), as the software strictly prevents over-votes and warns against under-votes. Furthermore, these machines are cost effective for helping the visually impaired as many not only have a headphone jack so that the blind can listen to the selections, but also other settings which allow for increased font size or other visual aids. These machines are also flexible in allowing many different length ballots or rules for each election on the ballot as it can be custom programmed into the ballot definition file and therefore can be changed right up to Election Day. This differs greatly from past paper ballot based systems in which the ballots needed to be printed ahead of time or lever machine systems in which the allocation of candidates on the machine needed to be decided far ahead of time to ensure enough switches for the candidates. They are also incredibly easy to use for citizens who don't speak English as they can be loaded with instructions in as many languages as the election official desires. In fact, studies on the added usability by Professor Charles Stewart III of MIT show that, "a DRE America would effectively enfranchise 250,000 – 800,000 more people (Tedeschi Autum 2006, 41)." User studies also show that people really like voting on the machines as the new technology feels more secure and feels "better." In

[4] This also means that later sections explaining the attacks against DREs will also work against dial DREs but only the attacks that ignore the user interface or presentation of the ballot will work against full-face DREs.
[5] In fact, one of the largest producers of DREs following HAVA was Diebold Corporation which makes ATMs and other banking equipment (S. Miller 2004).

fact, in 2009, when asked which type of voting system they prefer, 76% of voters who voted on DREs chose DREs and 48% of people who did not vote on DREs chose DREs (Stewart, Alvarez and Hall, Voting Technology and the Election Experience: The 2009 Gubernatorial Races in New Jersey and Virginia 2010, 9) and when given a choice between systems, 80% of voters in Fairfax County, VA chose the DRE (Epstein, et al. 2012).

That all said; there are some major weaknesses to DREs. For one, the DRE was simply a newer iteration of the Lever Machine. It provided over-vote protection and better usability for voters and ease for election officials to total the votes at the expense of transparency through the loss of a paper trail. Not only were DREs expensive and required the vendor's assistance to maintain (which produced much higher costs down the line than districts expected), but with DREs, the nation landed back in the era of blindly trusting the machine. The only record of a vote was the number on the removable media attached to the machine or the memory onboard the machine which made it impossible to audit the individual votes. Election officials again also had to trust the word of the vendors and rely on their forward deployed engineers to keep the election running. As Andrew Gumbel stated, "Not only did the manufacturers shroud their products in secrecy, but they also became actively involved in running elections, because technophobic administrators in many places thought having them around would help prevent mistakes (Gumbel 2005, 191)." This became especially worrisome given that the leaders of the election machine manufactures were deeply ingrained in the political process. For example, leading up to the 2004 election, Walden O'Dell, CEO of Diebold Inc., then one of the largest manufacturers of DREs, was a major supporter of then President Bush and even spoke at a rally for his reelection (Krugman 2003). However, as Rebecca Mercuri adeptly stated, "If the machines were independently verifiable, who would give a crap who owns them (Gumbel 2005, 247)?" Thus, the lack of any paper trail or verification process made the DREs a huge black box, swinging the needle of transparency (or more accurately, lack thereof) too far making it significantly easier for a covert attack to occur due to the lack of any potential exposure to detection from an audit.

In response, Vendors promised that their machines were secure, that their source code was well protected and therefore their systems were safe and secure from attacks. They lied. Not only were the systems insecure, but they were also incredibly buggy rendering them hard to use even if working properly. The Brennan Center for Justice compiled a "short list" of reported issues spanning the decade following the 2000 election for their paper "Voting System Failures: A Database Solution" and it covered 50 pages of the report (L. Norden, Voting System Failures: A Database Solution 2010, 46-96). The problems were so bad that in the Sarasota County CD-13 election in 2006 a 13% under-vote was blamed on touch screen insensitivity and slow response time (Mello 2011, 57). To put that number in context the highest rate in any neighboring county was 5%! Even worse it was reported that an internal memo had been circulated to the staff of the voting machine manufacturer three months before the election warning that some voters might press the button twice due to a delay in the graphic of the button press being registered and therefore de-selecting their choice and thus not voting (C. Thompson 2008), and that is exactly what happened! The lack of response or notification from the manufacturer can be traced back to the very long certification process for new machines, combined with the sporadic and relatively poor market for the machines (save the infusion of cash in 2002). As such, many of these companies were understaffed and not fielding the top talent and were desperate not to lose contracts. Therefore,

they were re-using code from past iterations and defunct machines, developing very slowly and not warning of potential problems. Instead they hoped problems would not show up before they could be patched in a future software update so that they could meet their deadlines. They didn't keep up with best practices in the industry, used outdated and unsafe languages, and used outdated hardware. This all led to machines that were brittle, hard to set up, hard to maintain, and not as user friendly to voters as promised. In short, America was voting on flip phones but being promised smart phones. Therefore, many of the theoretic usability gains from DREs were not realized and in many cases usability was decreased from these systems. To be fair, newer more updated machines have performed much better, but many of these usability problems still remain providing a cover for any attack that could simply emulate previously reported problems in the process of attacking the system.

Beyond the usability issues was a huge security vulnerability caused by the lack of transparency. Like lever machines, DREs operate as a black box and thus the software running the machine has to be trusted to work appropriately. Vendors therefore promised election officials that their software was secure and secret. However, following a quick Google search, Bev Harris, an owner of a small public relations firm in Seattle, was able to uncover the entire source code to one of the most popular machines at the time and one still used in a handful of states today, the Diebold AccuVote-TS (Gumbel 2005, 252).[6] Therefore, once this fact was made public, security researchers at various universities began to tear through the code to analyze it for flaws. And flaws they found. In fact, Professor Rubin of Johns Hopkins University and one of his graduate students were able to find a gaping flaw in only the first half an hour of analyzing the code (Gumbel 2005, 253). This trend continued throughout the rest of the professors who analyzed the code which led to a review of the code of many other DREs and all of them were also found to be equally vulnerable (Appel, Ginsburg, et al., Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine 2008, Calandrino, et al. 2007, McDaniel, et al. 2007, Yasinsac, et al. 2007).[7] Almost every machine was written with best practices thrown out the window, was open to various buffer overflows, and used encryption very poorly or not at all. The worst part was that many of these flaws had been pointed out to the various companies decades earlier during security reviews for certification and were never fixed (Gumbel 2005, 257). And with every one of the machines running the same flawed software, an attack that was found to infect one machine would be guaranteed to work on all of the other machines of its kind. This provides a tantalizing amount of scalability for an attack which was impossible with older systems. In short, the lack of transparency in the software design process and by the machines in action meant that votes could easily be changed maliciously or accidentally on a large scale and no one would be the wiser.

[6] The fact that this happened shows the fallacy of the idea that the code was secure because it was secret. Furthermore, Microsoft's Windows source code is kept secret but it is well known to not be secure, and that is despite the work of some of the brightest minds in computer science.

[7] This is only a partial list of papers to get the point across, but many others exist and many were referenced and reviewed in writing this thesis can be found in the bibliography.

Section 2.2: DREs with VVPAT, PCOS and Audits

"There is widespread agreement among security experts that some form of independent voter-verifiable record is critical for voting system security, and as a check against potential electronic miscounts (Goodman, Mulder and Smith 2012)."

Following the publishing of all of these flaws, the public was outraged and demanded a solution. The simplest solution that security researchers proposed was to ensure an auditable paper trail. Two solutions were proposed: retrofit the DREs with a paper trail, or abandon them and use the competing technology, the Precinct Count Optical Scanner (PCOS).

Whether it was due to accessibility concerns, lack of money, voter preference, or blind faith in technology, many counties opted to let the DRE manufacturers come up with a solution to the problem which they dubbed the voter verified paper trail (VVPT).[8] The way VVPT works is that when the voter finishes his vote and is at the review screen, a small thermal printer prints out a receipt summarizing the user's votes. This receipt is hidden under a protected transparent covering to allow the voter to see the paper but not be able to take the paper. Once the voter verifies that the paper trail matches the electronic display of the vote, that part of the receipt is either scrolled out of view or cut from the roll and dropped into a secure holding area to allow the next voter to vote without seeing any of the first voter's choices. If the voter thinks there is an error and chooses to change his vote then the current receipt will either print cancelled on it and scroll out of view or simply scroll out of view to allow the next confirmation to be shown. To many this seemed like the perfect solution. It provided voters with verification that their vote was saved correctly and an auditable paper trail. Election officials and the media at large were thrilled with the development. In fact, as early as 2006, in a referendum in Sarasota County Florida, voters overwhelmingly approved an amendment to ban any machine without a verifiable paper trail (Hansen 2012, 170).

However, computer scientists still cautioned that the VVPT was not a silver bullet. To begin with, the printer is still controlled by the software. Therefore, the printer could still be controlled to print false outputs or print the correct choice while the incorrect choice was saved to the electronic tally. Furthermore, the printers themselves are fallible mechanical contraptions. They can run out of ink, have a paper jam, or "accidentally" become unplugged from the machine. In these instances, voters could still vote but they would not have a paper trail to check and attacks could continue. In fact, these printer issues are not rare but have actually been quite commonplace in recent elections with some counties reporting failure rates of around 10% (Manning 2006). Furthermore, since the voting machine would know when the printer was connected and running properly, as it is controlled by the software, the attacker's code could know when the VVPT was working and tailor its attacks accordingly. Regardless VVPTs have been found to reduce the usability of the systems and led to complaints by voters to poll workers (P. Herrnson 2008, 128). In addition, the VVPT is printed via cheap thermal printers like the receipt printers from grocery stores which print in very small font. Some voters, especially the visually impaired or elderly, may not be able to check the results at all. Even then, it is conjectured that very few people check the paper trail and a recent study by Professors Ted Selker and Sharon Cohen of MIT calculated an error recognition rate of only 3% (Norden, Lazarus, et al. 2006, 66)! Furthermore, in

[8] In some cases it is also referred to as a voter verified paper audit trail (VVPAT).

personal conversations with young voters from Ohio, many stated that they never checked the VVPT or they didn't know that they were supposed to check it.[9] To make matters worse another study which tested whether people noticed mistakes on the review screen of the DRE itself found that more than 60% of the time mistakes went unnoticed (Everett, The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection 2007, ii). Thus, while the VVPT creates an accurate paper trail in theory, that is not necessarily the case in practice. To make matters worse, the VVPT may also compromise voter privacy as many systems use a continuous spool of paper which by definition retains the order of the votes. This enables a coercer to cross reference the votes with the order in which the voters arrived in order to determine which candidates each voter selected (Keller, et al. 2004). All of these downfalls with VVPT mean that DRE machines, while better protected from an attack with a VVPT, are still ripe targets for attack.

Largely due to these issues, many states opted for precinct count optical scan (PCOS) systems. PCOS systems are at their core very similar to the punch card systems and have been around since the 1950s (Jones, On Optical Mark-Sense Scanning 2010), but only recently became popular as the scanners were previously cost prohibitive. PCOS systems require voters to fill out a ballot by bubbling in the candidates on a pre-printed ballot and then feed them through an optical scanner which tallies the votes (similarly to the scoring of a standardized test such as the Standard Aptitude Test). The PCOS system has some distinct advantages over the Votomatic system and retained many of its desirable properties. PCOS systems by their nature have a paper trail as users vote on a paper ballot and are therefore auditable. Protections in system design prevent the short pencil attack from election officials, as voters are instructed to deliver the ballot in a manila envelope to the machine and feed it in themselves which never places the completed ballot in the election official's hands. At the same time, usability is quite high for election officials. Ballots are digitally scanned, allowing for a faster count and easier tallying for election officials, and election officials do not need as much technical know-how to run these systems. The system is also relatively cheap; polling places only need pens, privacy booths, and a single PCOS machine to count the votes (unlike the multiple DREs per precinct). Finally, absentee ballots can be designed to be identical to precinct ballots simplifying the ballot design process.

The biggest difference from past systems is that the votes are counted at the precinct. Individual scanners that also doubled as the ballot boxes are deployed to every polling place. While thus more expensive than simply having one counter at election headquarters for the entire district, the PCOS system has proven to greatly reduce the over and under-vote rates as the deployed counters are designed to reject ballots with an over-vote or under-vote and ask the voter to correct the ballot. This gives voters a chance to correct their mistakes which is not possible if the votes are tallied at election headquarters as the ballots are devoid of voter identifying information. Research by Professor David Kimball of the University of Missouri-St. Louis has found that switching from a central count to precinct count system will on average decrease the over-vote rate from 4.1% to 0.9% (L. Norden, The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost 2006) and thus saving over 3% of

[9] Names withheld for privacy reasons. N = 10.

the vote. In a populous county such as Los Angeles County that would mean that over 600,000 votes[10] could be saved by switching to such a system. As a final positive note on voter usability, the technophobic elderly have a much easier time voting with pen and paper than with the touch screen DREs. In fact, a 2008 study noted that PCOS systems resulted in fewer requests for help from voters than DRE systems (P. Herrnson 2008, 63).

However the system as released was not without its flaws. It was found that certain colors or types of ink were not being read correctly by many of the machines (Theisen 2009 , 3). Furthermore, some voters did not fill out the ballots correctly and just like on the SAT, not completely bubbling in the circle would often render the vote unreadable. PCOS systems are also not friendly to the visually impaired as they are still paper based systems. Precincts thus need to purchase additional systems such as Ballot Making Devices (BMD), which are essentially DREs optimized for the visually impaired that print out a ballot that can then be scanned by a PCOS machine. This therefore raises the cost of the overall system and requires poll workers to have to learn how to set up and operate two different types of voting machines. Also, there is no easy way to support multiple languages without multiple ballots. To top that all off these devices were not immune from bugs, errors and crashes. VotersUnited.org compiled a "short list" of errors and it was, like the DRE's "short list," over 50 pages in length (Theisen 2009). Therefore, the usability for voters can be greatly reduced.

Furthermore, the machines themselves could also still be hacked and the electronic records could be changed. After the election is over flash memory cards (like the cards used in digital cameras) are taken out of the back of the PCOS machines and brought to election headquarters for tabulation by the EMS. If at some point in the election these cards were swapped or before the election a bad card was put into the machine it could cause the electronic results to be incorrect or corrupt the EMS. Fortunately, however, with the auditable paper trail, a candidate could get a recount to reveal the true result. Also if there was a power failure the ballots could be stored in the emergency storage slot and counted later and there would be no slowdown in Election Day proceedings, although the advantages of precinct over central count would be lost. That said the system itself is pretty robust. Consequently, it is the recommendation of computer scientists that this is the best system on the market today as it is a private voting system that is transparent, with a fully auditable paper trail, is relatively low cost, is quite usable for voters, and is very usable for election officials. Therefore, it is also the hardest system to attack today.

Before this section is completed it is important to note that all modern systems provide on additional attack vector, the EMS. The election management software is the backend for any of the precinct deployed systems. It is software on a computer that initializes the removable media for all machines, sums the results returned by the removable media after the election and defines the ballots for DREs. If someone could get into the EMS then they could easily infect all of the machines in a given precinct. This is the largest disadvantage that comes with modern networked (even via removable media) technology. While, it makes administering an election much easier, as there is only once central system that has to be dealt with to update an election or sum and election, it means that there is a single point of failure.

[10] Based off of total county size of over 2.2 million in Los Angeles and thus 3% is over 600,000 votes (2012 California Presidential Results 2012).

While every lever machine in a given country would all have to be attacked individually, a single infected DRE or PCOS machine could send the infection back to the EMS via the removable media and then infect the entire county on the next election cycle. Therefore, the EMS is a critical piece to also consider when analyzing the security of the election, especially given that due to the ease it gives administrators, it is here to stay. Furthermore, since back in the Votomatic days and early optical scanner days central counting systems were used which also had a single point of failure, this type of threat is not new to elections and doesn't feel more dangerous to election officials. However, since many of the EMSs run on standard windows computers which are known to be vulnerable to attack and most removable media is often comprised of standard flash memory cards which can easily be infected, the risks are high and since isolation measures are not in place mass infection is a likely scenario (Halderman, et al. 2008).

As a final note, the advantages in security of PCOS systems over VVPT systems over pure DRE systems are rendered null and void unless the audits are actually done and done in a thorough and well-designed manner. If the precincts are announced before the election, or are picked by a non-random process, then an attacker can target the attack to subvert the audit. Good audit design, just like good voter registration design and good ballot design, while all out of the scope of this thesis, are very important for the security of the election. Furthermore, these audits are also not particularly costly to implement. In fact, in an election decided by 2% of the vote, only a 5% audit of all votes is needed to have confidence in the result and catch fraudulent activity (Norden, Burstein, et al. 2007, 21). Therefore, a good audit can render any attack that causes the paper and electronic records to differ, obsolete. That all said, if the chain of custody is lost and the ballots could be compromised, lost or replaced, the audit is useless. This chain of custody issue also arises with the vulnerable removable electronic media that stores electronic votes and the voting machines themselves in terms of what source code is running on the machines. Therefore, effective audit procedures and effective chain of custody procedures are key components of a secure auditable election process, and not surprisingly states around the nation are passing laws mandating such procedures (Norden, Burstein, et al. 2007, Lindeman, et al. 2008).

Section 2.3: Modern Trends: Early Voting and Vote-by-mail

"Citizens should not have to choose between waiting for hours to [v]ote or being disenfranchised (Verified Voting 2012)."

While PCOS and DREs with and without VVPT are the two main systems deployed in the United States today there are two other trends that need to be considered when analyzing the current voting system: first, the rise of early voting and second, the rise of vote-by-mail.

Early voting has some very positive traits. It keeps the polls open longer which allows people more flexibility in voting hours. This is especially helpful for those who are handicapped or those who work through Election Day. Furthermore, it gives the poll workers a couple of days to get used to the problems that arise during voting while the lines are short and delays are less costly. From a security standpoint it is also helpful as Election Day attacks affect a smaller percentage of the votes as the early votes have, in many cases, already been counted. In fact, in the 2008 election, over 13% of voting was early, in-person voting and this number was up from 3% in the 2000 election (Alvarez, Ansolabehere, et al. 2012, 36). At the same time early voting can be very dangerous from a security perspective. With early voting in place, machines must be moved into insecure polling places early. They are therefore left

potentially unguarded and exposed for many nights, the time at which the machines are most vulnerable (Epstein, et al. 2012) which increases the window in which attackers could gain physical access to the machines.

Vote-by-mail also adjusts the electoral process. In vote-by-mail systems, like the one in place in Oregon, all ballots are absentee ballots. Registered voters get their ballot mailed to them and then are asked to fill out the ballot and return it by mail to be counted via a central count scanner. This provides some amazing benefits especially for budget starved election administrators as with no voting machines to purchase or upkeep and no precinct workers to train the entire process is very cheap and simple. And, since modern mailed ballots are the same machine readable ballots used by PCOS systems, they are easily counted. This system ends up resembling a PCOS system but without the need to go to a precinct. Therefore, it is also very convenient to the voters who have time to contemplate their vote and send the ballot back at their convenience. Conventional wisdom states that this also allows voters to look up information on the smaller races and vote intelligently. Due to the convenience, low cost and paper trail, vote-by-mail is quite popular. In fact, its prevalence across the nation has been rising steadily by 3% for each presidential election since the 2000 election (Alvarez, Ansolabehere, et al. 2012, 36) and many states that don't have pure vote-by-mail systems still allow people in state to request an absentee ballot regardless of whether they are actually out of state. The system is also very useful because as Professor Philip Kortum of Rice University points out, users get to vote on a medium, paper, with which they are familiar (Stark, et al. 2012). Thus this system becomes user friendly in the same vein that PCOS systems are user friendly, with the added benefit that voters get more time to consider their vote and look up information on the candidates after receiving their ballot.

However, vote-by-mail is not without its flaws. For one, since the votes are tallied at election headquarters, vote-by-mail systems suffer the same over-vote and under-vote issues faced by central count scanning systems. Also many votes are lost since it is very easy for voters to forget to sign every box or fill out every bubble required to validate the ballot. Also, while many assume that the added convenience of voting from home will greatly increase voter participation and enfranchise many, evidence from the experience with vote-by-mail in California presents a counter example. As explained by the CalTech-MIT Voting Technology Project:

"A recent study – that took advantage of a feature of a California election that sets up a 'natural experiment' in which some voters are essentially randomly assigned to vote-by-mail one election but not the next – found that voters assigned to vote-by-mail were 13% less likely to vote, then voters who were allowed to vote in person on Election Day (Alvarez, Ansolabehere, et al. 2012, 42)."

While conclusions cannot be drawn from just one data point it is important to consider that the mythical gains from vote-by-mail may be just that, a myth. Vote-by-mail also relies on the United States Postal Service, a service that is not perfect and may lose votes in the mail, and is considering reducing its services making it harder for voters to get their ballots out on time (Stark, et al. 2012). Most importantly, vote-by-mail and absentee balloting in general is not really a secret ballot as there is no privacy booth and no election official around to ensure that voters get privacy and are not coerced. For this reason alone, MIT's Professor Ron Rivest, and many other professors around the world caution against these types of systems (Rivest, Thoughts On Appropriate Technologies For Voting 2012, Stark, Wallach, et al. 2012). In fact, vote-by-mail is the first system since the introduction of the secret ballot

over 100 years ago that sacrifices some voter privacy for other gains.[11] That said, it is very transparent (if one trusts the USPS and election officials to not violate the ballots), is relatively user friendly for both voters and administrators and is incredibly cost effective as no polling places need to be set up or manned, and is growing in popularity around the United States. Therefore, it needs to be carefully considered by the literature moving forward because, as David Wagner of University of California cautions, moving the pendulum too far in the direction of less privacy may lead to an incredible backlash and massive amounts of fraud and successful attacks (Stark, et al. 2012).

Section 2.4: The Voting System Today

"Our elections are so complex, and involve so many jurisdictions, varying technologies, voters, poll workers, technicians and election workers, that problems are inevitable. And, as the technology used for elections has become more complicated, the possibility of error has increased substantially (Goodman, Mulder and Smith 2012)."

Today's voting landscape is dominated by three different types of voting systems: DREs with and without VVPT, PCOS and vote-by-mail. The spread of these various systems around the United States forms a patchwork quilt at the state level and often at the district level as well. The final counts show that over 110 million registered voters use or have the option to use some form of DRE equipment, over 159 million voters use or have the option to use some form of optical scan equipment whether through a PCOS or vote-by-mail system, and a small but sizeable 12 million voters will be having their votes counted by hand (Verified Voting Foundation 2012).[12] This can be seen in Figure 6.

The voting landscape is also quite fragmented with over 16 companies distributing over 43 different models of their voting machines (Verified Voting Foundation 2012). Each different system in each category has specific advantages and disadvantages, but importantly, there has been a paper written by a computer security expert revealing the same types of flaws in almost every one. On top of that it is evident that audits, which many of the systems rely on for their increased security, while increasing in number and quality, only occur in a few states as seen in Figure 7.

After this exploration, an educated attacker's high level choices are clear: attacks against DRE systems will focus on their reduced transparency, attacks against PCOS systems will focus on their reduced usability, and attacks against vote-by-mail systems will focus on their reduced privacy and usability. Understanding the high level attack strategies to perform and how and why those strategies developed, the educated attacker would now seek to determine what all of the possible types of attacks are. That is what will be explored in depth in the next three chapters.

[11] Interestingly, it does not seem that the population at large is worried by these issues of privacy as in a 2006 survey over 40% of Americans wanted a receipt they could take home with them after voting which would destroy any voter privacy principles (Alvarez and Hall, Electronic Elections 2008, 142).

[12] While a few punchcard machines are still in use in Idaho, I will not consider them as only 65,000 voters have the option of using this equipment (Verified Voting Foundation 2012).

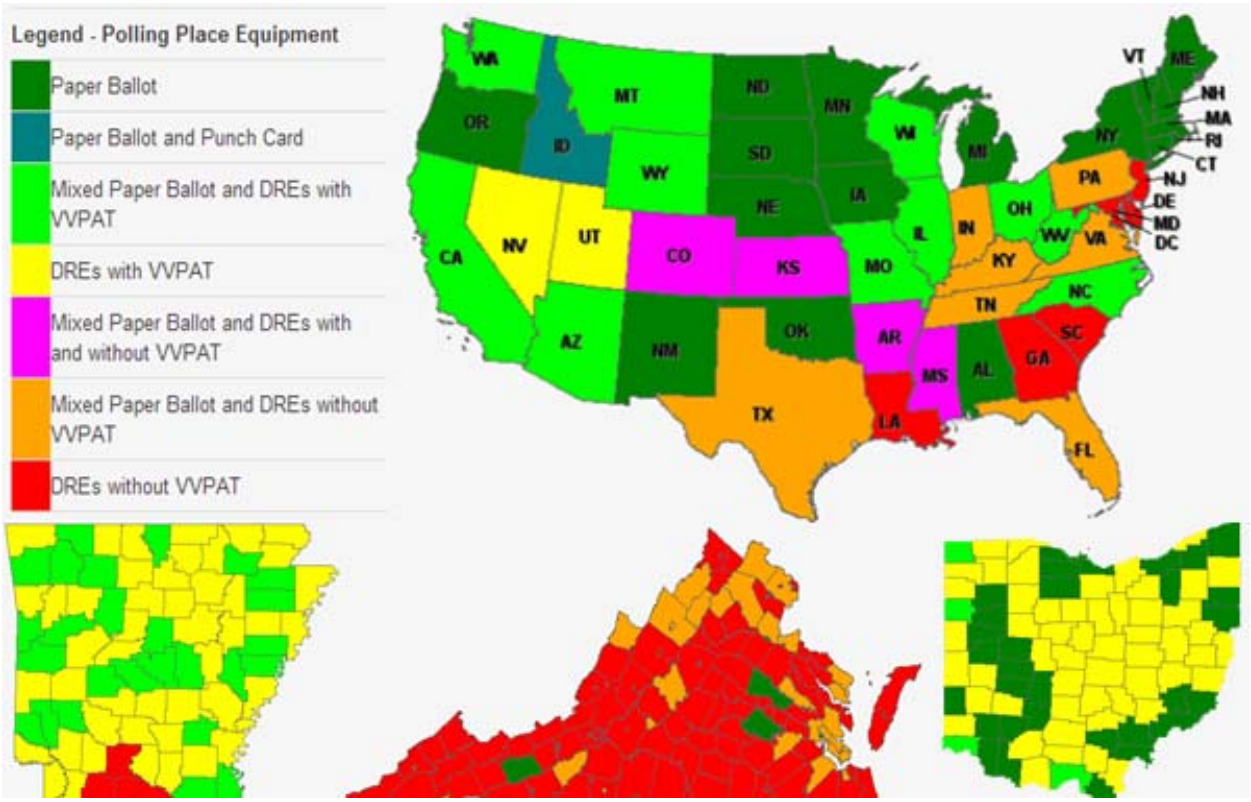

Figure 6: Voting Machine Distribution
(Verified Voting Foundation 2012)

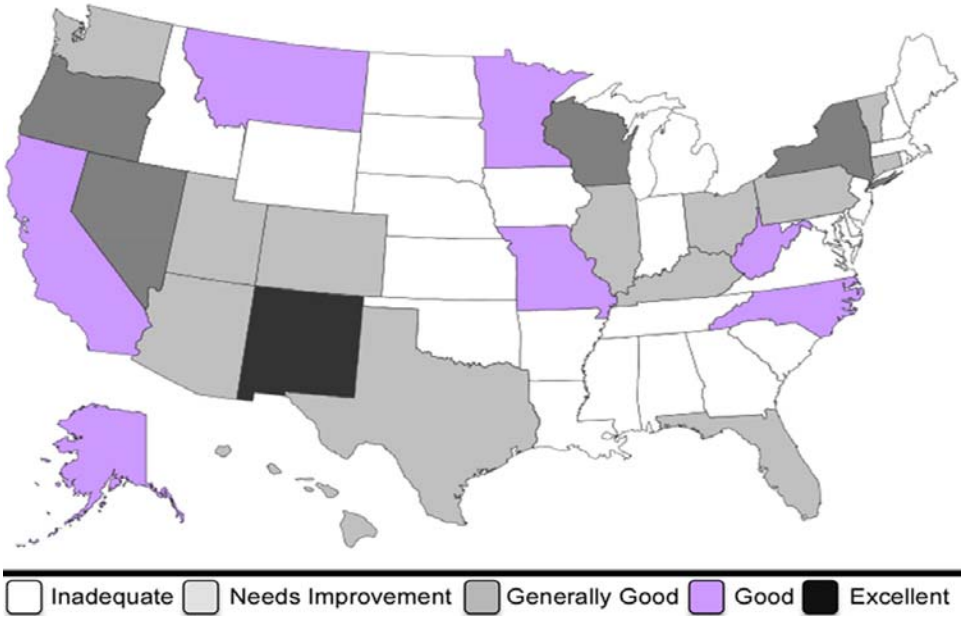

Figure 7: Audit Grades by State
(Verified Voting Foundation 2012)

Chapter 3: System Design Flaws and Attacks

"At different times in American history, the sanctity of the ballot box has been violated by intimidation, kidnapping, blood-shed, bribery, embezzlement, intoxication, under-the-table bargaining, stuffed voter rolls, creative vote-counting, and, above all, grotesque bureaucratic incompetence and corruption. Ballots have been bought and sold on the open market, stolen, forged, spoiled, and tossed into lakes, rivers and oceans (Gumbel 2005, 7)."

In beginning to explore the various attacks against the United States electoral system, which is laid out in the next three chapters, it becomes clear that the design of the environment in which the underlying voting systems operate greatly affects their security. Therefore, a detailed exploration of specific attacks against the modern voting systems needs to begin with attacks against the design of the larger system itself. Fortunately for an attacker, the complexity of the system enables many potential attacks that can shift the results of a vote without changing a single vote or hacking a single machine. This section describes the various system design attack vectors highlighting how effective each attack could be against each system according to its stealth, difficulty and assurances of votes stolen. The scalability issues with the various attacks are also explored. It is important to note that since votes are not changed, audits are useless against all of these attacks and thus audits are not considered. The attacks can be grouped into five categories: ballot design, voter registration, denial of service, physical access and pure politics. And in the end, while all of these attacks do not assure that a given amount of votes can be stolen or are quite difficult to achieve without detection, they can be potentially very powerful if executed correctly and thus need to be considered and explored.

Section 3.1: Ballot Design

"Two overriding lessons can be drawn from [the 2006 Florida Congressional District 13] election. First, that the design of voting systems and ballots can raise questions about the integrity of the process. Second, that the replacement of older technology with new, electronic voting systems and associated ballots does not remove that threat (P. Herrnson 2008)."

Ballot design can have a great impact on the outcome of an election. As mentioned earlier in the 2000 presidential election, many elderly voters in Florida were confused by the ballot layout and voted for the wrong candidate, likely swinging the entire election. Since most national elections and all presidential elections are decided across disparate and often incredibly partisan districts, one simply has to make a ballot that will cause voters in the partisan district that does not support one's candidate to either miss the race entirely or vote incorrectly in that specific race. As such, total votes for the opposition candidate will be severely reduced and the overall results could be changed. Past experience shows that this can be achieved in districts which vote on paper ballots, but can it be achieved in a DRE district?

In the 2006 Florida election in congressional district 13, the under-vote rate on the election for the House seat was an astonishingly high 14.9% in Sarasota County. This was very surprising for two reasons. For one, this was a high profile race and not only did lower profile races such as the race for the commissioner of agriculture registered only a 5.3% under-vote but also in the other four counties voting in CD-13 none of the under-vote rates were over 5%. Secondly, Sarasota County used state of the art DRE voting machines designed exactly to prevent the ballot design issues seen in the butterfly ballots and hanging chads of the 2000 presidential election. Therefore, given that the election was decided by only a total of 369 votes, foul play was immediately assumed by the losing candidate (Frisina, et al.

2008, Mebane, Revisited, Machine Errors and Undervotes in Florida 2006 2009). However, after much investigation it was determined that there was no foul play involved, that the machines functioned properly, and that despite the use of state of the art DREs, it was the ballot design that caused the issue.

The house election had only two candidates and on the Sarasota County ballot was placed on the top of the screen, crammed above the the large field vying for the governorship. In addition, the design failed to use differing coloring to indicate the race as was done in the other races on the ballot as shown in Figure 8. As such, many people simply did not notice the race, assuming it was part of the top banner of the page, and thus did not vote on the race (Doig and Tamman 2006). Similar high under-vote rates occurred in counties that had listed their attorney general election (which like the CD-13 congressional race had only two candidates) under the many candidates for governor further confirming this conclusion (Frisina, et al. 2008). In the end it was determined with over 98% confidence that had the ballot been designed correctly, the election results would have been flipped due to voting patterns in Sarasota County (Frisina, et al. 2008). Therefore, a ballot design attack is proven to work in practice and can swing an election whether the district is using paper ballots or DREs.

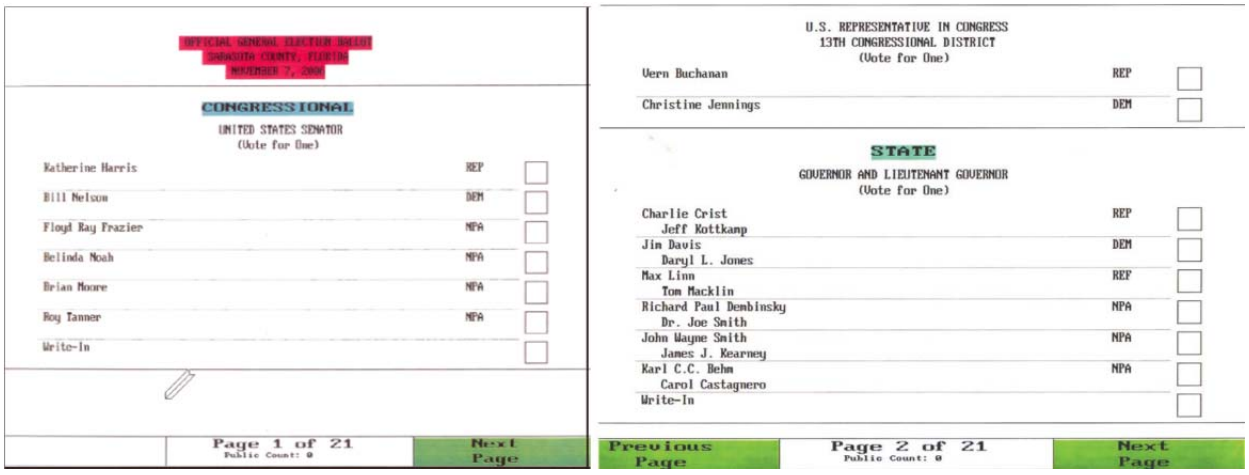

Figure 8: The 2006 CD-13 Ballot
(Ash and Lamperti 2008)

Despite the fact that the 2006 congressional race for the FL-13 seat was a high profile race, such a race is significantly less high profile than a presidential race. It is quite dubious that voters could miss a presidential race based on bad ballot design, or that the presidential race wouldn't appear as the first race on the ballot. Especially given that in presidential elections many voters come to the election solely to vote on the presidential election, such an attack should not be expected to have a meaningful effect on a presidential race. Furthermore, the attack would not scale very well as each ballot design is checked over by at least the election commissioner for each county prior to it being sent out to the machines. As such, many people would have to be involved in the attack making detection likely. That said, as exemplified by the CD-13 election, this attack could be very effective in a smaller race and could be used against all types of election systems.

However, this attack is unlikely to be an option for many more elections as many user interface design experts have begun working on analyzing user experience with different voter technologies and have

begun to draw up best practices for ballot design. In fact the Brennan Center for Justice distributed a report on the matter before the 2012 election (Norden, Quesenbery and Kimball, Better Design, Better Elections 2012). If election administrators ensure that ballots are designed up to these specifications and voters speak up if that is not the case, future deviations from good ballot design will be quickly noticed and not only will future accidental disenfranchisements stop, but this attack will also become easy to detect and thus very unprofitable to perform.[13] Therefore, through a little coordination and use of best practices, this kind of attack can essentially be thwarted in the future.

Section 3.2: Voter Registration and Authentication

"Voter ID, which is gonna allow Governor Romney to win the state of Pennsylvania, done." -Pennsylvania state House Republican leader Mike Turzai, June 23, 2012 (Wagner and Titus 2012)

Voter registration and authentication attacks are when voters are either enabled to vote multiple times or barred from voting unjustly. While these attacks are often the most discussed in the press, and can theoretically be most effective against vote-by-mail based systems, they do not scale very well and as such are not useful in stealing large national elections.

The voter registration system in America is known to be broken. The deceased, recently moved, and incarcerated often remain on the rolls. At the same time, those re-granted the ability to vote after serving their time are often left off of the rolls. This leads to the most commonly discussed type of voter fraud, multiple voting, in which people either register multiple times, in multiple states, or find ways to vote as other people on the rolls. However, despite the occasional case of a few non-citizens voting (Associated Press 2012), or people voting multiple times (Dicken 2012), this actually happens very infrequently. In fact, when the U.S. Senate Republican Policy Committee warned of voter fraud "plaguing" the nation's elections in 2005, the report was only able to establish that no more than 0.001% of votes are fraudulent and no more than 0.001% of elections are decided by fraudulent votes (Overton 2006, 162). Further research by Alvarez and Hall supports the rare nature of this attack revealing that between 1994 and 2002 there was only 1 allegation of fraud for every 975,000 votes cast and 1 conviction for every 1.3 million cast (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 90). Therefore, despite numerous claims of multiple voters, there is very little evidence of it occurring in practice.

This is due to the issue of scaling. If a person attempts to vote as many times as he can in a day, then under very generous assumptions he can at most vote 30 times.[14] Therefore, in the vast majority of elections, that many votes will not be significant enough to swing the decision. Furthermore, by voting that many times all the attacker needs to get caught are two people from different precincts remembering seeing him or her voting which is highly likely since the attacker would vote in precincts near his or her home precinct. If it is assumed that a person only votes 10 times, in order to reduce

[13] And while further exploration of optimal ballot design is out of the scope of this paper, a move to a standard national ballot design would also eliminate the learning curve for voters moving between districts or states.

[14] If a voter takes on average 15 minutes to vote (Stewart, A Data-Centered Look at the Election of 2008 2009), and if he needs to travel an average of 15 minutes to get to the next polling place (which is very generous given that in most of the United States precincts are very far apart, or in crowded cities), and if the polls are open from 5am to 7pm, thus open for 14 hours, then an attacker can vote at most 2 times per hour for 28 votes.

detection by traveling to slightly farther apart precincts, then to even swing the incredibly close aforementioned Florida CD-13 election, the attacker would have had to collude with over 35 different people. Thus, the odds of detection or betrayal are very high, and that is for one of the closest elections in the past decade. In most close national elections, decided by on the order of 1000 votes, on the order of 100 people would be needed to pull of the attack. Therefore, while it could be useful against small local elections, it is highly unlikely it would be effective in any national election and almost impossible in a presidential election. Furthermore, with the advent of open computerized voter registration databases, the rolls are continuously audited by special interest groups and invalid names are continuously removed from the rolls (Alvarez, Ansolabehere, et al. 2012, 26-28). As such, it is highly likely that one of these groups would spot a very suspect registration issue occurring in one part of one state and investigate further, making this even more difficult to complete covertly moving forward.

It is important to note that vote-by-mail and by extension absentee balloting greatly decreases the risks and increases the scaling ability of such an attack. With these systems in place attackers simply need to register a number of people who are eligible voters but either unregistered or not going to vote to an address at which he or she can covertly collect the ballots, fill them out, and send them back in. An often cited example of such an attack would be done by a worker at a nursing home who could register senile patients and vote for them. Furthermore, in vote-by-mail systems, many of the absentee ballots arrive on the same day to all voters as they are all sent out at the same time. Therefore, an attacker could simply drive down any street the day he or she received his or her ballot and steal ballots out of mailboxes. Especially when taking advantage of the uncaring or senile, these types of attacks are very hard to trace as many might actually not remember whether or not they registered to vote or even voted. Furthermore, all of the ballots would be legitimate ballots and thus no foul play could be seen offhand. Attacks from insiders can be even more dangerous as if one was an election official or someone with control over the database of the absentee voters, one could easily approve bogus absentee ballot requests in order to either execute an attack or aid an attacker.[15] Luckily, there are people who occasionally audit these systems and even fraud via absentee ballots can be noticed. In fact, Stephen "Stat" Smith, a state representative in Massachusetts announced his plans to resign in December of 2012 in response to allegations of these types of activities (Williams 2012). This proves that this type of attack is possible and can be successful in achieving its goal, but is hard to get away with.

At the same time the opposite type of attack can be made, denying valid voters the ability to register or vote. In fact, in the 2000 election registration problems disenfranchised 3.7 million voters or 2% of the voting age population (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 37-38). Fortunately, third parties are beginning to aid in the registration process and new online voter registration processes are being rolled out across the country reducing these issues.[16] That said, voters

[15] One could even have these ballots sent to a secure PO Box where he or she could collect them and submit them. Or, even more subtly, could input bogus addresses so the ballots were returned to sender and then the official could vote instead of destroying the returned ballots.

[16] Non-profit aid groups that help disenfranchised voters include the National Federation for the Blind (National Federation of the Blind 2012) and the League of Women Voters (League of Women Voters of Texas 2012). At the same time websites such as TurboVote are designed solely to make the registration and absentee balloting process

can still be actively denied the right to vote through the voter authentication process as this process varies widely by state. Requirements can be used in malicious ways to deny the vote to classes of voters that tend to vote in certain ways. In fact, if Virginia's law requiring a voter to either show a form of ID or to sign an affidavit in order to vote, was changed to always require a form of ID, the same type of law passed in Georgia (Office of the Secretary of State of Georgia 2012), over 9,000 people would have been barred from voting in the 2008 election for lacking proper identification (Stein 2012). This becomes especially poignant since many minority voters do not possess state identification cards and as such these types of laws could be used to selectively target minorities. Furthermore, shifting over 9,000 votes could have easily swayed the presidential race in Florida in 2000, the Governor's race in Washington State in 2004 and the Senate race in Minnesota in 2008, among others (Federal Election Commission 2001, Office of the Secretary of State of Minnessota 2009, Office of the Secretary of State of Washington 2005). As such, theoretically one of these laws could be used to steal an election.

Unfortunately for an attacker, such an attack requires the legislature and governor to be of the same political party that benefits from the action so that the law can be passed and requires that the courts don't strike the law down as predatory and unconstitutional. Thus, while Representative John Lewis of Georgia said in response the Georgia law, "It may not be the literacy test or counting jelly beans in a jar. People aren't being beaten or chased by police dogs, but it takes us back to another day and another period and as Americans we should not want to even dream about the past," Georgia was a state that was never in question for a presidential election and in all the states that are considered swing states, the laws were declared unconstitutional (Abdullah 2012)**.** Therefore, while these types of laws can be considered attacks and could swing some local or state elections, they will not be able to affect the election of a president.[17]

Section 3.3: Denial of Service

"I'm here to tell you, folks, you have got to stay bucked up. The effort to depress you and keep you home, I've never seen it like this before in my life." -Rush Limbaugh 2012 (Limbaugh 2012)

While the voter ID laws were unable to deny service to many voters, there are many other ways to perform a denial of service attack that are much more effective in disenfranchising voters and manipulating elections. Denial of service attacks can change the outcome of elections if they are able to deny the ability to vote to a subset of the population that is highly partisan.[18] The ability to shift elections be targeting partisan groups and districts is very powerful in a national presidential election, as the United States of America is a heterogeneous country with many pockets of highly partisan support. In fact, in a recent article, New York Times election statistics guru, Nate Silver, showed that due to

simpler and easier for all voters (TurboVote 2012). Finally, registration forms are now also available in both English and Spanish online (Alvarez, Ansolabehere, et al. 2012, 27).

[17] Also, these laws do prevent the rare multiple voting attacks. As such, they do also potentially provide benefits to the election process and thus are overall quite controversial.

[18] For example, if there are 105 people voting on the green and yellow candidates with 50 of them being from the rural population and 55 from the city with the rural population favoring the green candidate 4:1 and the city population favoring the yellow candidate 4:1, the yellow candidate should win 54 to 51. However, if for some reason 10 voters from the city could no longer vote, then the green candidate would now win 48 to 46.

gerrymandering over the past decade the United States has become increasingly partisan with each election (Silver 2012). Most denial of service attacks are simply centered on generating large lines to raise the opportunity cost of voting to the point where voters they choose not to vote. As such, these attacks can be quite covert as they will often appear to be flaws in the election system and not an attack. That all said, these attacks cannot guarantee that a definitive amount of votes will be stolen as voters may prove to be more or less resilient to delays than expected. As such, while they can be very powerful attacks, they are also quite risky as the variance of their effectiveness is quite large.

The first attack is to delay the delivery of voting materials. This would lead to longer lines as polling places would have to open late, force early voting to have to be canceled in certain districts, and make the return of absentee ballots impossible by Election Day. Systems that rely on a lot of absentee ballots can be impacted the most as whole swaths of voters could be completely disenfranchised in this manner. This is made even worse by the fact that the United States Postal System may be suspending service on Saturdays and thereby decreasing the window in which one can receive and send his or her ballot. This type of attack has already happened by accident at least once. In King County in 2002, absentee ballots were sent out so late that many did not have a chance to return them in time to be counted. Unsurprisingly, voter turnout was down to 53.2% from 74.7% in 2000 and 61.6% in 1998 (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 88-89). Since this attack has occurred in the recent past by pure accident, a future attack may be simply assumed to be another disasters error in election administration making this type of attack quite covert. PCOS systems are slightly insulated from the effects of this attack as they only need the paper ballots to be delivered to polling places by the morning of Election Day. As such, long lines, not disenfranchised voters would most likely result from this attack. That said, long lines can be devastating. In the 2000 election, issues with transportation and long lines at polling places discouraged 8.6 million or 5% of the voting age population from voting (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 37-38).

In the case of the King County disaster, the root problem was late submission of ballot design to the independent manufacturer of the ballots and delays on the manufacturers' end to return the ballots on time (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 88-89). Since a simple wrench dropped into one of the big printing machines could derail the production of the ballots potentially by days, reliance on outside manufacturers can open up whole new attack vectors. If an election official was in on the plot then simply causing disagreement on the final ballot design or ensuring there was a typo in the final ballot requiring a delay to fix the mistake could initiate the same type of overall delay in receiving ballots. Even if an insider was not in on the attack, the design could still be spoiled if an attacker intercepted the email or package with the final ballot design and instead submitted an incorrect ballot. If this was done subtly enough a candidate could be left off the ballot and this might not be recognized until Election Day which would be a disaster (although it is highly unlikely an election official would not notice a missing presidential candidate, this could work well in a small local election with a large field). Finally, an insider could purposely not order enough ballots for a city causing a crisis in the middle of Election Day resulting in lack of ballots for voters. The candidate who was counting on votes in that area would therefore have to immediately begin to attempt to round up voters, keep them at the polls, get a court order to keep the polls open longer, and re-round up more voters later at night to come back and vote once more ballots were obtained. While the last scenario

seems a bit farfetched, it actually occurred (although the lack of ballots was a mistake and not a malicious attack) in 2010 in Bridgeport, CT (Connors, Gendreau and Saperstone 2010). Again this creates the opportunity for a future attack to potentially appear as another terrible accident.

DREs do not rely on paper ballots, but are not immune from delays and attacks on the delivery and set up of the machines. DREs with VVPTs can have their VVPT function (and thus auditability) hindered or removed by similar delays in the production of the printer paper. This could have a huge impact on the election as while it alone would not change anything, removing the auditability of the election would open the DRE up to many software attacks (which will be discussed later). One could also derail the deployment and setup of DREs by causing problems in the warehouses that store the machines between elections. Causing the warehouse to have climate control failures, from things as simple as turning off the air conditioning to flooding the floor by leaving a sink on in the bathroom, could damage the machines requiring replacements at the last second. Since the voting machine business is a sporadic one, manufacturers do not have a plethora of machines in stock (Gumbel 2005) and as such delivery of a sufficient number of machines could be impossible. As such, early voting could have to be suspended in certain areas and fewer machines could end up being delivered to precincts. Consequently, lines in precincts would balloon, and as mentioned above, discourage voters from voting. Also, air conditioning systems break and buildings flood for various reasons all of the time which could again make the attack appear to be a tragic accident. One could also intentionally poorly calibrate the machines during their initialization. This would lead to very frustrated voters who take a significantly longer time to vote, attribute the problems to bad touch screens (which they interact with all the time given the ubiquity of bad touch screen interfaces seen today), and cause the lines to grow exponentially. This attack is made even more effective as buggy machines have to be taken offline all the time (Jauregui 2012), and lines are known to occur frequently at polling places (Overton 2006, 44).

DREs also offer other venues for denying service to voters due to the fact that most current machines are completely reliant on a steady power supply and can only remain active for very short periods of time on battery power. In fact, many of the machines' batteries can only last up to two hours before the machine crash from lack of power (Ansari, et al. 2008). With no other voting option available to DRE based precincts, voting would have to be suspended until power could be restored. To make matters worse, if some machines were not shut down properly then the previous votes made on those machines earlier in the day could be lost. This would occur because many of the machines store their votes in their random access memory which is lost when a machine loses power. The only solace would be if the DRE had a VVPT which could be used to reconstruct the earlier votes. Therefore, the DREs lack of adequate battery power could provide a very effective attack vector, especially considering the prevalence of power outages around the United States. In fact, in 2008, the Lake Tahoe region of California suffered a power outage which took all of their electronic voting machines offline (Howard and Slabaugh 2008). Fortunately for that election, the region was using PCOS machines. As such, voters were able to vote on the paper ballots and simply store their votes in the emergency ballot box on the PCOS machine to be scanned later. This illustrates why DRE machines are much easier to attack through this vector, although one would be amiss not to note that in this case the aforementioned 3% reduction in over-votes would be lost since votes would now be scanned centrally.

While all of these types of denial of service attacks are interesting in theory, in order to understand more about their effectiveness one needs to understand whether voters will actually be dissuaded from voting by long lines, delays and inconveniences. Intuition suggests that many voters would be dissuaded but evidence of voters sticking around in lines lasting multiple hours indicates otherwise (Damron and Hall 2012). Fortunately for an attacker, Hurricane Sandy provides a very nice proxy. Falling only days before the election, many voters were denied the service that they expected. Due to the storm the New Jersey voting infrastructure was decimated. In the end while many braved the reduced service, longer drives, and longer lines, overall voter turnout in New Jersey fell to a recent record low of 60%, 10% less than the previous low in 2000 (Baxter and Bureau 2012). This shows that these attacks if done properly and cause enough disruption, could be expected to dissuade 10% of the electorate, and since these attacks affect all types of elections equally, they could be useful in attacking a presidential election. Of course, it is unclear if the depressed voter turnout from Hurricane Sandy was mainly due to longer lines at polling places or due to the fact that many voters were trying to figure out how to salvage their homes, get to a location with working heat and recover from the destruction. As such these attacks cannot be guaranteed to dissuade a large amount of voters.

Section 3.4: Physical Access Attacks

"Requiring that voter-verified paper audit trails be added to DRE voting machines to detect error or fraud will not provide complete security in an election because the integrity of the election still depends on the chain-of-custody remaining secure (Castro 2007, 9)."

Beyond simply denying service to the system one can also begin to effect change on the system by attacking the chain of custody of the ballots and the removable media. This can be done to directly affect the system or to obscure other types of software based attacks that will be discussed later. These types of physical attacks include: stealing the removable media cards used to store the ballot totals in DRE or PCOS based systems, stealing the paper trails, whether the actual ballots in a PCOS system or the VVPTs in a DRE with VVPT system, and attacking the mailed in ballots in a variety of ways to influence their result before they are fed into the central scanner. While these attacks can be quite powerful and greatly affect election results they are also quite risky as they are likely to be detected.

Figure 9: CF and PCMCIA Cards
(McDaniel, et al. 2007, 47-48)

Modern voting systems rely on electronic counts and removable media to enable a quick and accurate count of the votes. When the polls close, removable media is taken from each machine and brought to election headquarters where they are inserted into the EMS for final tabulation. This happens regardless of whether the system is DRE or PCOS based. In most cases the removable media used is either the

standard compact flash (CF), Secure Digital Flash Memory Cards (SD cards), or PCMCIA SRAM flash cards used by most modern digital cameras and cellular telephones phones shown in Figure 9. (McDaniel, et al. 2007). The ubiquity and small size of these types of removable media devices provides a cheap and convenient option for election administrators, but also make them ripe for attack from malicious insiders and outsiders.

To begin with, given their small size and generic nature, these devices could easily be stolen before, during or after the election. Before the election the cards are initialized on the EMS to hold the ballot definition file (on DRE systems) and are primed to store the counts from the votes. They are then placed in packets with all of the instructions for each precinct and held at election headquarters until the day of the election when they are distributed to the election official heading up the process at each precinct along with ballots (in PCOS systems) and other Election Day materials (Registrar of Voters Association of Connecticut 2011). At this point the packet could easily be accessed and the memory cards could be easily swapped out or tampered with by a corrupt election official, especially since it has been shown that the tamper resistant seals are not actually tamper resistant at all (Appel, Security Seals on Voting Machines A Case Study 2011). Furthermore, outsiders with information regarding the location in which these packets are stored (which is usually election headquarters, although the handbook for Connecticut only requires that the materials "Should be stored in a locked storage location not generally accessible (Registrar of Voters Association of Connecticut 2011)"), through some simple breaking and entering, can have full access to a precinct's removable media prior to election day and can steal, break, tamper with, or swap out the removable media. That said, "simple breaking and entering" is quite a dangerous action and one that has a high potential rate of detection, which is why insider attacks are more powerful.

Insider attacks are also more powerful after the election as insiders are required to transport the memory cards back to election headquarters. Again the security of the removable media is reliant on good chain of custody procedures by election officials and the security of the insecure seals, and as such election officials could easily tamper with the vote totals on the removable media devices. Again election officials could be mugged and the cards could be taken by an outsider, but again this is a highly risky maneuver. The most likely outsider attack would be to attack the memory cards while voting during the day and conveniently for an attacker, many of the machines have the memory card slot easily accessible to the voter. As such, the card could be removed and replaced with a new card by a voter during the day. To make matters worse most machines do not authenticate new cards and will simply accept the new card with whatever information it possesses (McDaniel, et al. 2007, 130). Since the cards hold vote totals and the ballot definition files, an attacker could delete or alter votes from earlier in the day, insert new ballot designs which could be missing candidates, or could cause the machine to crash taking it offline and increasing the size of lines in the precinct. Even worse, an attacker could insert a Trojan horse in the removable media which would infect the EMS when the removable media was inserted into the EMS for tabulation after the polls were closed (this type of software attack will be explored in greater detail in the next chapter). In short, insiders can greatly affect the election by attacking the removable media, and while outsiders can as well, it is a much riskier proposition.

Similar system attacks can be made on the paper trails. As discussed, in both PCOS and DRE systems, the paper trail can be used to audit the election results and ensure that no software based attacks can

actually change the outcome of an election without the potential of detection through a mismatch in the paper and electronic totals. However, just like the removable media, the paper trail needs to be transferred from the precincts to election headquarters or the storage facility in which they are kept. This again provides a large amount of time in which the paper can be stolen, altered, or ruined. Again, insiders have a much greater opportunity to attack the paper trail as they are entrusted with transporting them around and responsible for properly sealing them and guarding their integrity. Attackers could also attack the VVPT printers to ensure that they do not print legible paper trails. In fact, it has been shown that if some simple household chemicals are accidentally inserted into the printers in the beginning of the day, which could easily be mistaken for a poor cleaning job, the VVPT will become illegible as shown in Figure 10.

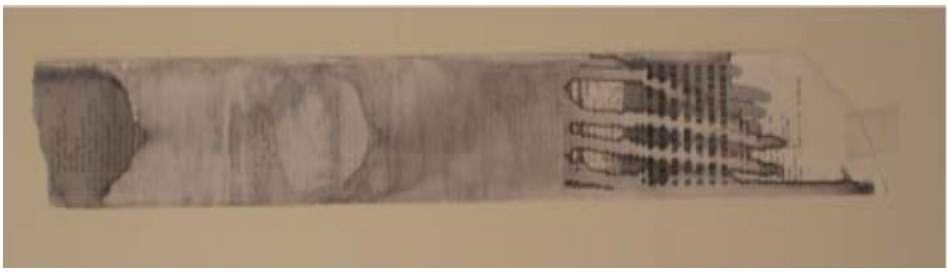

Figure 10: A Spoiled VVPT Printout
(McDaniel, et al. 2007, 186)

Historically, attacks against the ballots in transit before they were tabulated have been commonplace. There are many stories of ballot boxes found dumped in rivers and streams, or stories of dumpsters full of shredded ballots. In fact, in 2001 votes from a San Francisco referendum were assumed to have been dumped into the bay as ballot box lids were found floating in the bay days after the election (Gumbel 2005, 13). Relative to attacking the removable media, however, these attacks are very risky. When attacking the removable media, an attacker can deploy silent software attacks by infecting and replacing the original pieces of media back into the election process. Replacing the paper trail with duplicates with different results on them cannot be done with equal speed, accuracy, or stealth. Furthermore, for a ballot box to be "lost" a true accident must be set up with the delivery car, as in the modern age no one would believe that ballots could just disappear and appear floating in the river later that day. This again shows the importance of paper trails as they are much harder to attack and can help prevent or at least discourage other types of attacks as they will retain the true counts.

The most likely attack vector is an insider attack on the reams of paper that make up the paper trail while it is stored in its post-election storage facility which can be used prevent an audit. This facility may in many cases simply be a storage area which can be accessed easily and can provide an attacker with time to carefully swap out the paper trails or cause a fire sprinkler to accidentally go off and ruin the paper trails. Even still this type of attack could only succeed if the attacker has some time to destroy the paper trail before the audit took place. Proper prompt auditing will again make this type of attack exceedingly difficult to perpetrate without detection. And while there is precedent for this type of attack as it appears that in the recent election someone tampered with the final paper voter records in Fulton County Georgia, prompt review of the documents after the election caught and fixed the error showing how difficult it is to complete such an attack covertly (Edwards 2013).

Mailed in ballots provide a longer time frame between voting and tabulation creating many more opportunities to attack the ballots both before and after they arrive at election headquarters. Since the ballots are routed through the postal system on their way to election headquarters, simply having an accomplice in the mail sorting room can make disenfranchising voters simple and since individual voters who vote via absentee or vote-by-mail systems are never notified if their vote is received, a few key missing votes here and there are unlikely to be noticed. All an attacker needs to know is the destination address for the mailed in ballots, which is publically available. Then the attacker can selectively choose to have certain ballots get lost in the mail. The lack of security from seals means that careful attackers can potentially unseal envelopes, check the vote, and reseal them and either send them along or remove them depending on the vote on the ballot. At the same time some simple statistics can be done as well to prevent an attacker from even needing to open the envelopes as votes coming from a highly partisan counties, towns, or universities can be removed safely knowing that one would be stealing significantly more votes from one candidate. In fact, one would not necessarily even need to work in the mail sorting room of a big mail center to perpetrate such an attack, one could simply be the mailman who delivers the ballots to election headquarters, or one could simply distract the mailman and take the ballots out of the back of his truck. These types of attacks are not safe by any means as an overwhelming amount of mail being lost may arouse suspicion, but it can be done through much more publically accessible areas than an election official's car on his way to election headquarters. Furthermore, many ballots are not returned by voters or do get lost in the mail as in the 2008 election over 21% of all requested absentee ballots leaked out of the system before counting even began (Alvarez, Ansolabehere, et al. 2012, 42). Thus, there is a strong precedent for a large amount of absentee ballots never reaching election headquarters which may provide cover for such an attack.

Beyond stealing the ballots themselves, there are many other potential insider attacks that can be made on the mailed ballots themselves through their validation process. A prime example of validation manipulation is the bitter contest between democratic challenger Al Franken and republican incumbent Norm Coleman in the 2008 Minnesota senate election. The race was close enough that absentee balloting totals determined the result and therefore the standards on what constituted as a legal absentee ballot determined the outcome of the race (Wall Street Journal Editors 2009). Consequently tense fighting occurred over whether a missing signature on the inner envelope or a stray ink mark on a ballot invalidated the ballot. In such environments, selective application of acceptance criteria can easily help steal or add votes to one candidate. Furthermore, election officials could add stray marks or bubble in a second vote on peoples' ballots who voted for certain candidates in order to invalidate the vote. Therefore, careful observation of election proceedings by members of both parties needs to occur. Furthermore, while it is highly unlikely that people will choose not to vote in a presidential election but vote in lower elections, many lower elections are likely to be left blank by many voters and as such, election officials could fill in those votes for the voters who left the race blank and influence the outcomes. Fortunately, most districts have both a Republican and Democratic head election official who together oversee the entire election process and as such the presence of members of both parties in the room should make such attacks unlikely and very likely to be detected. However, if correct procedures are not followed or if one election official suddenly became ill (by accident or on purpose) and there was no plan in place to have a replacement brought in, such attacks could potentially be easily perpetrated if

one person was left alone with the ballots before the tabulation was done. Again this is a very risky attack vector but with the growing use of vote-by-mail, it is an attack vector which may grow in importance over time and must be considered. In the end while all of these physical access attacks are quite risky, they can be quite powerful and also show how corrupt election officials can greatly affect the outcome of an election.

Section 3.5: Cutthroat Politics as Usual

"If you do everything, you'll win." –Lyndon Johnson (Gumbel 2005, 1)

The Minnesota senate race shows a glimpse of how the political fighting around close elections can be both intense and evoke a win-at-all-costs mentality. This type of mentality often inspires some individuals in major positions to commit what may be downright fraud or at least actions that smell quite fishy. While such actions can often only occur in special circumstances and are often quite risky and overt, they must be considered. The best recent example comes from a 2002 election in Alabama. As Andrew Gumbel explains:

"Take, for example, the governor's race in Alabama in 2002, when the Democratic incumbent, Don Siegelman, appeared to have won by a narrow margin, only to be undone by the sudden discovery of a computer glitch in rural Baldwin County. The count's probate judge in charge of elections had taken it upon himself to check the tabulation machinery in the dead of night, long after poll workers and most of his staff had gone home, and concluded that Siegelman had accidentally been awarded seven thousand votes too many – enough to tip the entire race to his Republican challenger, Bob Riley. County officials were distinctly vague about the cause of the supposed error, furnishing no details other than a passing reference to a lightning strike. Of course, it may have just been a coincidence that the judge was a Republican, just as it may have been unimpeachable legal precedent that led Alabama's attorney general, also a Republican, to refuse authorization for a recount or any independent inspection of the ballots. A subsequent analysis of the voting figures by James Gundlach, a sociologist at Auburn University, showed all sorts of wild deviation from the statistical norms established by this and previous elections." (Gumbel 2005, 8-9)

Whether or not actual wrongdoing was done in Alabama in 2002 it is painfully obvious that many politicians are willing to do whatever it takes to win, and while a purely political attack on a presidential election would be nearly impossible such attacks could be quite useful against smaller elections.

As this chapter has shown, when analyzing attacks against voting machines it is important to also take into account attacks on the larger voting system. Poor assurances of a strict chain of custody of sensitive materials, poor design of ballots, poor guarantees of continued service to voters and insider attacks can result in compromising not only ballots and paper trails but also individuals ability to vote. This failures can directly lead to tainted election outcomes. While many of these attacks do not guarantee victory or actually change results and are quite risky, many of these attacks can provide a springboard from which other attacks can be used to change an election result. The one big takeaway that must be drawn from this chapter is that insiders are powerful and systems need to be designed to reduce their power and ensure that checks on their actions and decisions are in place through well designed audit methods. Otherwise an attacker could use key officials' aid to sway elections.

Chapter 4: Software and Hardware Attacks on the Voting Infrastructure

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts." -Gene Spafford (Dewdney 1989)

As powerful as system design attacks can be, it is the threat of a software enabled attack that changes votes and ballots in real time that keeps security experts up at night and conspiracy theorists actively blogging. These attacks can be on the physical hardware or purely on the software and can be initiated in various time frames from as early as months before the election to during Election Day. This chapter seeks to explore each of these attacks making sure to keep audits in mind as some of these attacks can be discovered through audits. This chapter first covers background on software and hardware attacks, explores the various flaws found in modern voting systems that allow for these attacks and finally dives into the various software and hardware attack schemas.

Section 4.1: Computer Security Background

"Today, major security breaches dominate headlines on a weekly basis. Intrusion campaigns such as 'Operation Shady Rat' (disclosed by McAfee in August) and 'Nitro' (disclosed by Symantec in October) show a systematic compromise of every significant sector of the economy including technology, industrial manufacturing, defense, financial services, and government and nongovernment organizations. In addition to the systematic compromises of these sectors, we've seen hints of cyberwarfare operations including Stuxnet, Duqu, and the recent loss and capture of the US RQ-170 Sentinel spy drone over Iran (Ghosh and McGraw 2012)."

Over the past ten years cyber-attacks have grown from sporadic attacks perpetrated by a few rebellious hackers to a multi-million dollar criminal industry with focused and sophisticated attacks occurring daily. Furthermore, many nation states have developed sophisticated cyber warfare capabilities. As Ghosh and McGraw point out, attacks against major companies seem to be mentioned in the news every day and the companies that are being attacked include those dedicated to computer security and firms that design the security schemes of some of the government's most secure networks. In fact, recently the top secret plans to the brand new Joint Strike Fighter, amassing several terabytes, were covertly syphoned off of "secure computers," and the Air Force's air traffic control system was hacked (Gorman, Cole and Dreazen 2009). Scarily, all the information and software needed to perpetrate many of these attacks is fully available online. Full penetration testing suites designed to infiltrate corporate networks and used by many network testers such as the Metasploit framework are downloadable for free (Metasploit 2012). Youtube videos can guide would-be hackers through step by step instructions on how to send a self-deleting virus (Josh 2007). Simple Google searches result in troves of information. As such, the current climate is quite a dangerous one and companies are not prepared to defend themselves. As Richard A. Clark, a former cybersecurity expert for President Bush, told corporate executives in April 2002, "You will be hacked. What's more, you deserve to be hacked (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 79)."

Furthermore, while software is written in human-readable coding languages, it ships as massive files filled with byte code. As such it is very difficult to go through the thousands of lines of just zeros and ones and track down every potential malicious line of code that was inserted into the software. Even by diffing the software against a known good copy, simple changes in the compiler optimization level, the platform upon which it was compiled, or time at which compilation occured can lead to a multitude of

false positives making detection often difficult and tedious. Even worse, the compiler could have been swapped out for a malicious one that inserts the malicious code at compilation time making it almost impossible to recognize the error unless the compiler itself was examined. Ken Thompson, in his Turing award acceptance speech, went a step further and actually inserted a backdoor in the UNIX operating system by instructing the compilation of the compiler to insert code that would cause the compiler to insert the backdoor into UNIX when it compiled UNIX. As such, only by examining the source code of the compilation of the compiler could this backdoor be discovered (K. Thompson 1984). With all of these many ways to sneak malicious code into software it is almost impossible to ensure that the software will behave appropriately and given the large amount of bugs often found in code, and the fact that many mistakes are purely accidental, it is incredibly difficult to determine if an attack is occurring or if the software is simply highly flawed.

Given this environment, many voting machine companies have resorted to security by obscurity. They have foolishly believed that if no one has access to their source code then it will be very hard for anyone to figure out how to attack as disassembling the distributed binary would be prohibitive. However, this ideology has been proven to be inneffective as the source code for many machines has shown up on the internet as mentioned earlier (Kohno, et al. 2004) and a machine itself was even listed for sale on eBay® (Calandrino, et al. 2007, 10). Even if the source code is not mistakenly leaked, it lives on the companies' servers, servers which can easily be assumed to be insecure given the rash of break-ins to many major defense contractors over the past couple of years. Therefore it is not obscure. This faulty belief has ensured that security researchers have not been given access to the software and as such have not been allowed to analyze it for flaws. However, in the few instances in which security researchers have gotten their hands on the source code, the reports have been incredibly damming.

Section 4.2: An Overview of the Key Software Flaws

"Paperless electronic voting machines cannot be made secure." –National Institute of Standards & Technology (Percy 2009, 29)

Voting machines today are highly flawed and as Professors Kohno, et. al. put it in their 2004 paper, "We see no evidence of disciplined software engineering practices [in any of the source code] (Kohno, et al. 2004, 4)." The code is not only written in unnecessarily outdated languages full of non-memory safe functions leading to buffer overflows, integer overflows and illegal array accesses, but is also written with bad coding style leading to duplication of code and poorly scoped variables. The code also shows a lack of understanding of cryptography and often inherits many flaws from the other software with which it is bundled. As such, the machines today are highly vulnerable to a multitude of software attacks.

Many of these security flaws arose because companies tried to re-use as much code as possible from older iterations of the machines to save costs. Since much of this code was written before security was a major concern, the code is riddled with security flaws. To make matters worse, many of the flaws in the code were pointed out to the companies years earlier in security reviews but were never fixed. As the Brennan Center for Justice noted, "Wired and Computerworld Magazines have reported that the voting system vendor was aware of the 'Deck Zero' problem [which cause the first batch of absentee ballots to not be counted in many districts] for years, but did not notify the election assistance commission, the national association of state elections directors, or the California secretary of state, California's chief

election official (L. Norden, Voting System Failures: A Database Solution 2010, 12).” Therefore, the Brennan Center for Justice has called for a database of voting machine failures and issues in order to help ensure accountability on the part of the voting machine vendors.

Regardless, many of these flaws are easy to correct and would have never existed had the company decided to re-write much of the code in a more modern language instead of sticking with the original outdated and non-memory safe language. For Example, ES&S’s full fleet of voting machines including PCOS, central count scanners, DREs, and the EMS systems are written in a total of 12 programming languages with nearly 670,000 lines of code of which 63% is written in memory unsafe languages such as the ancient COBOL and notoriously memory-unsafe C programming languages (McDaniel, et al. 2007, 34,83). This has led to the use of many non-memory safe and outdated library functions such as `sprintf` and `strcpy`, and combining this with the vast amount of code, has led to a situation in which buffer overflows are omnipresent. Sadly, programmers were often aware of these problems but chose to ignore them. Comments in the source code point to this mistake as shown below:

```
340: Assume buf is large enough for a token
341: This would be better if it delt[sic] with CStrings
342: rather than with fixed buffers. Gems implemented
343: this at one point.
```

This comment not only points out the flaw but states that the company had fixed it at one point but for some unknown reason chose to stop using the safer version of the code (Calandrino, et al. 2007). The ubiquity of these flaws provides an attacker with a lot of power.

This occurs because by exploiting a buffer overflow an attacker can gain full control of a machine because the coder used a function which blindly copies as much memory as it is given to a destination address. This is highly problematic if the destination address is a variable sitting on the main memory stack. Since memory is filled from the bottom up, this extra-long input will (if its length is not checked, which these non-memory safe functions choose not to do) first fill the space allocated for it and then keep extending up the stack overwriting whatever was previously there. If the input is of the correct length it can extend far enough up the stack and overwrite the return address of the current function which will break the logical flow of the program and instead direct it to execute code at whatever address the attacker specified. In fact, a crafty input can have the logical flow return to a specific part of the attack code itself allowing the attacker to dynamically insert new functionality into the code. Therefore, through the use of a buffer overflow an attacker could instruct a machine to change its vote totals (One 1996). And, fortunately for an attacker, buffer overflows have been found at every point input is entered into modern voting machine systems whether it is the code that reads the ballot definition file (Yasinsac, et al. 2007, 57) or the code on the EMS which reads in the vote totals from the removable media (McDaniel, et al. 2007, 53). The widespread failure to check for buffer overflows continues for other main types of simple but deadly security holes such as integer overflow vulnerabilities (same basic principle but overflowing a number input instead of a text based buffer) and array out of bounds accesses (again similar principle but this time abusing the fact that if the code goes to the “ith” entry in the array, a malicious coder could tell it to go to an “i" value which is outside the

size of the array and thus have the function access arbitrary data) (Yasinsac, et al. 2007, 57).[19] As such the machines are incredibly vulnerable to a software based attack despite that fact that they could have simply been secured by writing the software in a more modern memory safe language such as Java, and without a very large performance penalty, especially considering how bad the performance already is today. Attackers everywhere could not be happier.

These machines have also been coded for convenience of the coder without regard to potential security consequences. Two glaring examples lead to ways in which an attacker can tell if the machines are being tested or actually being used. In this way an attacker can instruct his attack code to have no impact on the output and performance during testing and then unleash the attack during actual voting circumventing even the best pre-election testing standards. The first way in which this can occur is through the clock. There is no real need for a clock with the actual date and time on the machines. As Professor Aviel D. Rubin explains, "Without a clock a programmer could not write malicious code to trigger at a specific date or time, like on the morning of Election Day (A. D. Rubin 2006, 182)." Maybe if one wanted to print out timestamps on a VVPT one could have a local clock that is only accessible by the printer, but there is no need for a globally accessible clock. In many cases this was left in the software because the software was built on other free or publically available software which already had a clock and the coders did not spend the time to remove it. This pure laziness added a dangerous flaw to the machines. The other more subtle issue arose from the testing mode installed in the machines. While testing mode is designed to emulate the actual voting experience, it is often different in some subtle ways in the code. For convenience, the coders installed, in many cases, a global variable to indicate whether the machine was or was not in testing mode (McDaniel, et al. 2007, 75). Therefore, the voting machine software can simply check the flag and proceed accordingly. Of course the attacker can do the exact same and only proceed with the attack if the flag indicates that it is not in testing mode. This flag did not need to be globally accessible but for coder convenience was made so. These two oversights are therefore great examples of poor design of the code on voting machines.

The code on these machines also displays a complete lack of understanding of modern cryptography. Cryptography is used in these devices to ensure that the vote totals and audit log data stored on the machines and removable media cannot be accessed and manipulated by an attacker to ensure integrity and voter privacy. Most machines do use some cryptography and occasionally use checksums to check for unauthorized access and manipulation, which is encouraging at first pass. However, the manner in which this cryptography is implemented is so poor that it makes it completely irrelevant. In fact, in their 2004 study, Khono et. al. discovered that every single Diebold machine used the same hard coded encryption hash key shown below.

```
#define DESKEY ((des_key*) "F2654hD4")
```

By exploring the source tree they were able to determine that the line that defined the hash had not been changed since at least 1998 (Kohno, et al. 2004, 14)! As such the encryption was a complete farce as pretty much anyone who had ever worked on the code or reviewed the source code knew the

[19] A more detailed explanation of memory based security issues can be found in Randal E. Bryant's *Computer Systems: Programmer's Perspectives* (Bryant 2010).

passcode to decrypt the data on every single machine. In more frightening news, it turns out that this critical flaw had actually been pointed out to the company in 1997 by Professor Doug Jones of the University of Iowa during a source code review, but his dire warning was ignored (Kohno, et al. 2004, 15). Further exploration of the encryption decisions continued along this scary trend. In fact, the DES encryption standard that the code used had already been demonstrated to be insecure and easily broken via a brute force attack years earlier. The source code also included the following comment:

```
//LCG – Linear Congruential Generator – used to generate
        ballot serial numbers
// A pseudo-random-sequence generator
//(per Applied Crpytography, by Bruce Schneier, Wiley 1996)
```

It then went on to use a LCG for cryptographic purposes even though the paper they sighted in the comment explicitly warned against ever using the LCG for cryptographic purposes (Kohno, et al. 2004, 14-16). These types of flaws are also not unique to Diebold machines and these types of errors and damming comments are found throughout the source code of various vendors. In fact, the ES&S iVotronic encrypts the data on its removable media, but uses the data that is passed in cleartext on the removable media to define the key and as such all data can be trivially decrypted (McDaniel, et al. 2007, 58). The AVC Advantage is even worse in that it, like the Diebold software, uses some insecure checksums and hashes; however, the results cartridge doesn't even check them and simply uses the plaintext files instead and as such the encryption is completely irrelevant (Appel, Ginsburg, et al., The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine 2009, 13). In short, the lack of understanding of cryptography and terrible implementations on voting machines ensure that nothing is actually encrypted and therefore no voting data is actually secure.

To top things off, much of the code is simply copied and pasted around the code base making duplicate code common (McDaniel, et al. 2007, 62). As such, flaws in some of the duplicated code end up being fixed in one copy but not always in the other copies. Vulnerabilities are allowed to persist in the code base despite the fact that they have been noticed and solutions have been designed. In conclusion, while these are not the only oversights in the code base, these are large, glaring and easy to fix errors that serve as prime examples of the sloppy and poor code found running modern voting machines.

Many of the systems also rely on commercial of the shelf (COTS) software as a backbone for the systems and thus expose themselves to all of the flaws present in the COTS software. While the use of COTS software makes sense for the company from a potential cost cutting strategy and time saving strategy due to the reduced amount of software that the company needs to write (especially since some of the backbone software such as operating systems are difficult to implement), it means that the voting machine is now vulnerable to every flaw found in the COTS software. The is especially scary for the machines running on outdated versions of the Microsoft Windows operating system as they are known to have many critical security flaws. These flaws include many of the previously mentioned memory and scoping vulnerabilities and other issues that can lead to an attacker being able to gain root access on the machine and therefore have total control over its actions. For example, ES&S's EMS, Unity, runs on Windows XP (McDaniel, et al. 2007) which is widely known to have critical security flaws especially if the Service Pack 2 update has not been installed. In fact, Windows XP before Service Pack 2 is so vulnerable

that many introductory books on hacking use it as the environment to begin to learn how to hack a computer (Seitz 2009). Furthermore, most machines use standard types of removable media such as SD cards to transport the vote tallies and ballot definition files, and standard plug-and-play units on the circuit boards such as the PROMs (Programmable Read-Only Memory Units) to store the firmware that is central to the machines operation. Due to the standardization of the hardware, attackers can easily gain identical hardware in order to practice their attacks.

That all said, many voting machine companies have experimented with custom reduced instruction set languages and custom removable media, but errors in their designs make them equally vulnerable. ES&S designed for its flagship product, the iVotronic DRE, a ballot definition file delivery system based on a custom piece of hardware called a Personal Electronic Ballot (PEB). A PEB communicates with the iVontronic via infrared light and unlike the standard memory cards many other machines use, the PEB could not be obtained at any electronics store and had to be ordered directly from ES&S. Unfortunately, given the custom nature of the device inadequate protections were made to sanitize the input coming from a PEB as the ES&S software developers assumed that all information coming from a PEB could be trusted. This led to a very powerful attack vector if a PEB could be stolen and reprogrammed which would not be that difficult given the vast amount of PEBs used in elections. Even worse, it has been shown that there is an easier way to emulate a PEB simply using a standard Palm Pilot and a magnet. One can then give bogus instructions to a voting machine to gain complete control of the machine, or vote an arbitrary amount of times (McDaniel, et al. 2007, 50,66). Therefore, the custom hardware of the PEB provided absolutely no added security to the iVotronic. On the software side, Diebold designed a custom programming language which it called `AccuBasic` that it used in its AV-OS PCOS voting machine. Like the PEB this custom programming language was designed to improve security since all attack code would need to be written in `AccuBasic`. Not only would this require attackers to understand the custom language, but it was also supposed to render all attacks benign as the language was designed specifically to be sandboxed by the firmware to operate in a read only manner. However, Kiayias et. al. were still able to code up a piece of attack code in `AccuBasic` which would not only strengthen other attacks against the machine but would also be able to bias the election results in order to ensure a chosen candidate would win the election (Kiayias, Michael, et al., Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting 2008). Therefore, whether a system is using COTS or custom software and hardware, the machine is incredibly vulnerable to attack.

Before this section concludes, it is important to make two notes. First, despite the fact that some of the reports cited in this work are a couple of years old and as such some vendors have claimed to have patched many of these noted flaws in the intervening years, history shows that the vendors are more likely than not to have instead neglected to make these changes. Even if they did, given the ubiquity of flaws in popular COTS software which is often put through serious security reviews and rigorous testing, I believe it is safe to assume that other equally damaging mistakes could be found in the code base. Secondly, while removable media attacks can theoretically be used to attack both DREs and PCOS machines, these attacks are much easier to preform against DREs. The defining difference is that in the case of PCOS machines, the EMS only sends the machine an initialized piece of removable media to store the vote counts. It is not entirely clear if the PCOS machine ever tries to read any data off of such a piece of removable media during normal interaction and as such it is not clear if as many exploits can be

initialized by the machine during its normal procedures. However, in the case of DREs, the EMS also sends along a ballot definition file which the DRE needs to read and interpret in order to function. As such, the DRE assures an attacker that it will read and examine all of the data in the ballot definition file which provides an optimal location to store a command that begins the installation of the attack code. Therefore, all removable media attacks considered throughout this paper are much more effective against DREs. That all said, all of the forms of removable media on all of the types of machines have been shown to be vulnerable to attack and can lead to attack code being deployed to the system, the question is just how much interaction an attacker needs to have with a machine to make this occur.

Section 4.3: Attack Profiles

"To advance irresistibly, push through their gaps." – Sun Tzu (Tzu 2012)

Given the ubiquity and variety of software flaws explored in the previous section, it is fairly safe to assume that any machine is vulnerable. Therefore, the next question is: what specific types of software attacks could be perpetrated against the system, and what are the pros and cons of each attack? This section seeks to answer that question by providing a synthesis of the main attacks discussed in the computer security literature as well as other attacks that I invented.

Attack 1: P + -P = 0. The first attack is to insert some code into the machine that attacks the zeroing out of the vote totals[20] before the election. The code would ensure that a correct zero tape[21] would be printed to prove that the totals are zero and the machine is primed for voting, but then set the initial electronic vote totals to P and -P. In this way at the end of the election 2P votes will have been shifted from the -P candidate to the P candidate[22] and the vote totals will still be equal to however many voters entered the precinct that day since P + -P = 0. The code would also be instructed to delete itself right after it rigged the starting counts in the election ensuring that the only evidence of any malicious activity on the machines before voting began would be the incorrect starting electronic vote totals. Since those totals were just "confirmed" to be correct by the zero tape, no malicious activity would be assumed. During voting nothing different would occur. The only change would be that at the end of the day, the vote totals would have 2P votes shifted to the P candidate. Unfortunately, with a simple audit of a paper trail, it would be clear that the paper totals and the electronic totals were different and that 2P votes were shifted. Consequently, this attack is only truly viable against a DRE system without VVPT. However, this attack could still be performed against any system as long as an audit is not performed against the attacked votes. That said there is one other large threat for detection that must be mentioned. If P is set to too large of a number, the huge shift would probably be noticed as a statistical oddity, but more importantly, the -P candidate might end up with a negative vote total, immediately raising alarms. Therefore, this attack cannot be done (at least with a non-small P value) in areas that have a highly variable amount of voters or in areas that have very few voters for one candidate. Code could be left on the machines to check for this case and correct the error so that both totals were positive but that

[20] Setting the totals all back to 0 and clearing all data in preparation of a new election.
[21] A print-off showing that the original totals are all 0.
[22] This of course assumes 2 candidates, but in the current American political system there really are only 2 parties and thus 2 candidates and for president this is almost always the case. Either way this can be extended to 3 candidates but for simplicity I will assume 2 candidates.

would defeat the entire purpose of deleting the attack code from the machine so early in the voting process; the main benefit of this attack plan.

Attack 2: My Commission is X%. In this attack the attack code is designed to shift X% of the vote from one candidate to the other. This could be done as the votes are tallied by having an X% chance of each vote for an opponent being switched in the electronic count or at the end of the election by en masse switching X% of the opponents electronic vote total when a poll worker selects the close the election command. This would overcome the two shortcomings of *Attack 1* as it would ensure that a certain percentage of the vote was switched, preventing too large of a percentage of the vote being switched and would only switch those votes if they were available, preventing a case of negative votes. Thus it is much safer in those regards. However, it still retains the same audit dangers as it also only changes the electronic totals. It is also more dangerous than *Attack 1*, as it leaves the attack code on the machine throughout the election as the code can only delete itself when the close election command is selected (in either vote switching method). As such, attack code is left as a "smoking gun," exposed on the machines for a much longer amount of time. This is a large issue as precincts around the country close at different times which could lead to a situation where an early closing precinct throws out an alarm and a late closing precinct's machines could be inspected before the trigger for deletion of the attack code occurs. While a well-designed attack would presumably not arouse suspicion fast enough for such a situation to occur, it is still possible and definitely must be considered.

Attack 3: Presentation as Misdirection. This attack is an augmentation on *Attack 2* that is designed to circumvent audits on DREs with VVPT by exploiting the fact that the VVPT printer is in the end controlled by software which tells it what to print. A software attack can therefore alter the printout as well as change the electronic counts. This attack proceeds identically to *Attack 2* by changing X% of opponents votes as they come, but also causes the VVPT to print out the incorrect vote which is being recorded in the electronic count, while leaving the review screen on the DRE showing the voter's intended selection. This means that while the DRE screen shows who the voter thought they selected; both the paper audit trail and the electronic count say otherwise preventing detection from an audit. This attack does still remain vulnerable to detection from the fact that the code stays on the machine until the election is closed. However, more importantly, this attack requires that people do not check their VVPTs and notice that they were incorrect. However, as previously mentioned, it appears that only 3% of voters actually notice these errors and many don't even look at the VVPT at all. Some machines also have a moveable flap which when closed, fully obscures the VVPT printout which could be intentionally closed by an attacker or accidentally by a voter and thereby decrease the detection rate even further (Calandrino, et al. 2007, 5). As such, very few people would be expected to notice the discrepancies.

That said, even a few people who cannot get the machine to vote correctly would immediately lead to detection. Therefore, in order to appease the people who notice the error, the code would be designed to allow a voter to vote correctly if they went back and tried to fix the error. Given the buggy reputation of the machines, it is quite safe to assume that if the machine functioned normally on the second try, the vast majority of people would be fully appeased and would chalk the issue up to a small bug or maybe their own error (maybe they read one of the two screens incorrectly). Even if they did choose to complain, if the code was designed to shift 10% of the overall vote given that only 3% of those attacked

notice the attack than only 0.3% of people would notice in total. Assuming in the worst case that all 100% of them were not appeased only 0.3% of people would not be appeased on the correct second attempt, and given that on average a DRE services at most 300 voters (Alvarez and Hall, Electronic Elections 2008, 39), then each machine would be projected to have 1 complaint each day. Therefore, if the fact that many voters will be appeased is brought back into the fold then the inverse of whatever percentage one believes will be appeased is the percentage of machines that will receive complaints for that kind of mistake in a given precinct on Election Day. Given the many errors that were noted earlier to have come up on the past couple of elections and given the fact that the vote worked the second time, it is very likely that the poll worker will chalk the voter's complaint up to voter error. Therefore, this is an incredibly powerful attack that is likely to go unnoticed during the election and will circumvent the "voter assuring" audits in states with DREs with VVPT.

Taking this attack one step further, an attacker can take advantage of the speed at which the printer can print and scroll the VVPT paper and still attack someone who checked to make sure the VVPT had the correct vote. In order to do this when a voter confirmed the vote and pressed the final submit button, the machine would, in one quick motion, cancel the vote, print out the new vote, and submit it. While this type of attack has proven to be possible to implement (McDaniel, et al. 2007, 94), this attack would be easily caught if any voter was able to read fast enough to notice what was occurring, or recorded the VVPT on his or her smartphone.[23] Therefore, while potentially very effective at switching votes, this iteration of the attack would also be highly risky.

Security researchers have also pointed out that while the iterations of this attack will get passed the most basic audits, if one was to track the amount of canceled votes during the audit then this type of attack would be noticed (Norden, Lazarus, et al. 2006, 70), as all of the cancellations in votes (or an overwhelming majority of them) will correspond with votes only being switched from the attacking to the attacked candidate. That said this defense fails for a couple of reasons. For one, an informed attacker would be aware of this check and would therefore attack some voters who voted for his preferred candidate as well to generate cancellations in the other direction. He would do so by not only shifting the electronic and paper records but also displaying the incorrect vote on the review screen. Therefore, as previously discussed over 40% of those people would notice and switch their vote registering cancellations in the other direction at a much higher rate. Therefore if the total cancellations were designed to even out, then overall drastically more votes would be stolen than given away. The only data that could then be drawn from the audit would be that there were an uncharacteristically large amount of re-votes indicating that the machines were not working very well that day. This would make it impossible to draw any conclusions as to which side the attacker was working for, or if an attack even occurred at all. Also, even if something was noticed, the attack code would have been deleted as well since the code deletes itself at the close of the election, well before an audit could be performed and analyzed. And, the cancellation statistic is not currently being collected and as such is not a concern for an attacker today. Thus, this attack still remains a very potent and effective attack on a DRE based

[23] In fact, one voter sent out a smartphone recording of a touchscreen bug on a machine in Ohio in the 2012 election (Jauregui 2012)

systems with VVPT and audits as it only relies on voter ignorance, something that appears to be in no short supply.

Attack 4: Run Away! This attack takes advantage of the fact that if a voter does not complete the whole voting process and does not click the final submit button on a DRE then the voter is legally considered a "fleeing voter" and in many states, the vote must be discarded. Through this rule voters can be attacked in two different ways. First, when a voter actually flees the attack code can switch their vote to the attacking candidate and submit the ballot for them, thus registering an extra vote which will appear to be 100% legitimate. As there is no voter present, this will work whether or not a VVPT is present as no one will be there to check the paper trail. While fleeing voter rates are relatively low at 6% in one lab experiment (Everett, Greene, et al. 2008, 887), this will still ensure that all of the 6% of those votes are given to the attacking candidate. A second possible attack is to cause legitimate votes for one's opponent to be turned into fleeing votes and discarded. As the EVERSET report explains:

"If a voter does not select the candidate that the attacker wants, the malicious firmware intercepts the confirmation page's confirm function and pretends to cast the ballot: the normal 'thank you' page is displayed but nothing is printed on the audit tape. After waiting a few seconds (during which time the voter likely leaves the booth) the firmware again displays the confirmation page. After some time, the firmware calls the fleeing voter code and the machine will start chirping. A poll worker will think the voter was a fleeing voter, and, in accordance with Ohio's procedures [and procedures around the nation], the ballot will be canceled (McDaniel, et al. 2007, 95-96)."

This will therefore steal votes from the opposition. It is important to note that this attack again relies on voter's ignorance and the lack of attention they usually pay to the VVPT. Therefore, this is more effective in non-VVPT systems and has a potential for detection by cautious voters who diligently check their VVPT. Therefore, in order to appease voters, as in *Attack 3*, if a voter waited long enough to see it return to the review screen, or if the voter went and got a poll worker because the VVPT wasn't printing anything and attempted to confirm the vote a second time, the confirmation would work. Therefore, the attack would entail similar risk/reward properties of *Attack 3.* Given the relatively low fleeing voter rate, this attack could not be scaled to attack a very large percentage of the population as the statistically significant increase in the fleeing voter rate that would ensue would become suspicious. However, attacking one legitimate voter for every fleeing voter would keep the rate the same and cause a potential 12% swing in the election which would cause significant damage. That said it is dubious that during a real election voters would make as many mistakes as during a lab experiment due to the increased focus on the part of voters. As such this 12% number is probably quite high. However, even if this number was four times too large, 3% of the vote could be changed on DREs which could still greatly impact an election.

Attack 5: All Votes are Not Created Equal. This attack takes advantage of the fact that DRE only systems use the same DREs for both provisional and normal votes. Provisional votes are votes cast by voters who do not appear on the voter rolls of the precinct at which they show up to vote. Under law such voters must still be allowed to vote but the vote must be tagged as provisional. After the election the eligibility of the voter is then examined in detail and the vote is either accepted (usually because the voter went to the wrong precinct in the same district, or the voter rolls did not include his or her name by accident) or the vote is discarded. In this attack the attack code takes advantage of the fact that often one in four

provisional votes are discarded (Herron and Smith 2012)[24]. Therefore, whenever a provisional voter votes for the attacking candidate the code marks the vote as a normal vote and replaces a normal vote for the attacked candidate cast with a provisional one instead. In this way all provisional votes for the attacking candidate are marked as normal votes and are not at risk of being discarded. However, normal votes for the attacked candidate take on the risk of those provisional voters. Therefore a swing of one half of the total amount of provisional votes will be enacted by the attack. This attack is also not likely to be discovered as currently districts do not keep records of discarded votes. Even if noticed it would likely appear that the attacked candidate was trying to bump up his vote totals by sending in a large amount of ineligible voters to vote for him or her making this an incredibly effective and covert attack. However, this attack is predicated on there being a large amount of provisional votes which varies greatly per state. And while in Ohio, one of the states with the most provisional votes in the 2008 election, almost 3.5% of the vote was comprised of provisional ballots, many of these ballots were cast on paper as well as on DREs (Mears 2012) and the national provisional voting rate in 2010 was only around 1.5%. Therefore, nationally it can be assumed that at most 1% of votes will be provisional votes on DREs. While this is not a huge number, switching half of that rate or 0.5% of the vote could potentially swing a very close race or at least aid in other attacks. Therefore, this can be an effective attack.

One final note on attacking DRE voters is that the attack code has the added advantage of being able to selectively target voters that it feels will be more naïve and likely to not notice the attack being performed against it. This can be done by having the attack code target voters who take a very long time to vote or who access the help menus on the DRE (Calandrino, et al. 2007, 16). This can therefore reduce the risk of detection even further and while the percentage of voters who have trouble and would fulfill this criteria is unknown, this can only help the attack.

Attack 6: I knew I forgot to do something. This attack takes advantage of the previously mentioned fact that when there is no over-vote protection (and by extension under-vote protection), voters are much more likely to make a mistake and the rates of errors in votes rise drastically. Therefore, turning off the over-vote protection feature on a PCOS machine or programmatically disabling the over-vote protection and under-vote warnings on DREs could be expected to increase, on average, the amount of spoiled ballots by the previously mentioned 3%.[25] This type of attack is very hard to detect as it doesn't actually change any votes but simply takes advantage of the bad ballot design in United States elections and the incompetence or inability to understand the confusing ballots by many voters. Furthermore, many PCOS machines have the option to turn off their over-vote protection. This has even been done in a real election including the 2000 election in Escambia County, which unsurprisingly led to increased over-vote rates that equaled neighboring counties that used central count scanners (Mebane, The Wrong Man is President! Overvotes in the 2000 Presidential Eleciton in Florida 2004, 527). Therefore, an attack could potentially be assumed to have been a mistake by election officials. The code can also delete itself right after the election starts, just like *Attack 1*, as the over-vote protection mode is enabled as part of the initialization. One must however remember that it is highly unlikely that a voter will over-vote or under-

[24] And in some extreme cases such as in North Carolina in 2008, over 50% were discarded (L. Norden, Issue Brief: Election 2012 Recounts 2012, 23).

[25] And in some extreme cases it could even result in an increase in errors in almost 9% of the vote (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 36-37).

vote on a presidential election, but if the ballots are designed poorly enough, anything is possible, and the 2000 election debacle is a clear example of that conclusion.

Unfortunately, on DREs this attack is much less covert and its effectiveness is unknown. This is because DREs are programmed to prevent over-votes. As such a record of an over-vote will immediately cause alarm making it very risky to allow over-votes on a DRE. Furthermore, no studies have been performed on what over-vote rates would be on DREs if thy were allowed. Thus there is no guarantee that the 3% added over-vote rate will occur making it a high risk gamble to allow over-votes on a DRE. Removing the under-vote warnings, on the other hand, might be a very fruitful endeavor especially to aid a ballot design attack against a certain race. However, again, it is very unlikely that under-votes will occur in a presidential race and thus this attack is not very useful on DREs.

Attack 7: Oh that's what you meant. Another attack which focuses only on PCOS and vote-by-mail systems is an attack against the reliability of the scanners used in the PCOS machines and the central count scanners used in vote-by-mail systems. This attack takes advantage of the fact that there have been many occurrences of these scanners being unable to read certain kinds and colors of ink and being easily confused by stray marks. In fact, in a 2006 Orange County election, votes were lost due to the fact that the scanners could not read the gel inks used in many precincts (L. Norden, Voting System Failures: A Database Solution 2010, 12-13). If an attacker recalibrated the machine to reject any ballot as an over-vote or under-vote that voted for the attacked candidate and has any deviation from the normal standard, even those generally considered passable (and in the case of a PCOS system layer this on top of *Attack 4* to prevent any notification of this event), the attacker could invalidate votes for the attacked candidate. However, this attack still relies on voters to make errors on their ballots, errors that usually fall in the range of 1%-5% (L. Norden, The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost 2006). One could strengthen the attack by choosing to also mark as an under-vote or over-vote perfectly legitimate ballots that voted for the attacked candidate. This attack would now be quite noticeable via an audit as the electronic and paper records would differ and there would be no stray marks to explain the difference, but would be very effective in states without audits. However, with regards to both this attack and *Attack 4* one has to be very careful with causing a spike in over-votes and under-votes as since the 2000 election this statistic has been tracked carefully by the Caltech-MIT Voting Technology Project (Alvarez, Ansolabehere, et al. 2012).

Attack 8: The Big Switcheroo. This attack takes advantage of the fact that many polling places and districts have quite partisan vote totals. In these areas the spread in votes between the two candidates can be substantial, often reaching as high as 20%. In this case attack code that caused the machines to flip the candidates' vote totals could lead to a dramatic shift in the race. There are some serious problems with this attack however. For one, an audit will immediately catch the attack as the paper trails and electronic records would differ. More importantly, if a serious underdog suddenly won an election by a huge margin this would be a huge red flag. Therefore, this attack would actually be most effective in a district with: a margin of victory projected to be around 5%, no audits, and one using DREs so there would not be a paper trail to check at all even if a recount was instituted. In this way it would be unlikely that the attacking candidate would come out with a surprise victory (and then lose due to the fact that the totals were switched), but it is also realistic that a surprise victory could occur. This

attack could also be made safer by having the attack code check the final vote totals and if the attacking candidate actually pulled the upset victory then the votes would get switched back. With this augmentation in place, this attack now becomes more effective the smaller the margin of victory, as the switch becomes increasingly believable. At the same time, if the margin becomes too close an automatic recount will be instituted in most states and if the paper trails exist and do not match the electronic totals, then the attack will be caught. That said in certain instances this attack can be quite powerful.

Overall this chapter has shown that there are a variety of different flavors of attacks that can be perpetrated against the various voting systems with different pros and cons. It also becomes clear that the most powerful attacks can be done against DREs as the explicit paper trail in PCOS systems renders many attacks null and void, or at least voidable through auditing.

Chapter 5: Getting the Attack Code on the Machine

"When a single entity, such as a vendor or state or national consultant, runs elections or preforms key tasks (such as producing ballot definition files) for multiple jurisdictions, attacks against statewide elections become easier. Unnecessary centralized control provides many opportunities to implement attacks at multiple locations (L. Norden, The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost 2006, 32)."

Even with vulnerable software and the correct attack code, the hardest part about attacking the current voting system is getting the attack code onto the voting machines. This may seem counterintuitive in today's age of constant cyber burglary all over the internet. But that statement itself holds the key to why attacking the voting system is much harder than attacking online retailers; the ease of attack is predicated on the fact that both sides are attached to the internet. Unfortunately for attackers, the current voting systems are almost always isolated from the internet and for the most part machines are also isolated from each other. As such, one cannot simply preform the traditional hacking techniques of probing the servers of the company to try to find a weakness, fuzzing the inputs and gaining access. This provides a huge security benefit to the current systems in place and makes the attack much more difficult. That said there are a variety of ways to get the exploits onto the voting machines and each has different pros and cons which will be explored in this chapter. In short, moving from attacking individual machines, to districts of machines, to a whole company's fleet of machines makes scaling the attack much easier but makes getting the attack code on the machines themselves much harder.

Section 5.1: Individual Machine Attacks

"Simply slapping seals on a device does not magically protect it. Physical seals in general can be defeated with simple techniques and at low cost (Appel, Security Seals on Voting Machines A Case Study 2011)."

Attacking individual machines can be quite straightforward and these attacks could be performed before or even during the election through either removable media attacks or through gaining physical access to the machines ahead of the election. This makes this access vector quite flexible and covert. However, this access vector does not scale very well.

Voting machines are often stored in generic warehouses in between elections. They are not closely guarded and are rarely monitored. This occurs for two main reasons. For one, cash strapped districts do not have the funds to pay for high security storage facilities[26] and often do not have enough space in town halls or other government buildings to store the machines there. Even still, most government buildings are not that secure to begin with due to this same funding issue. Simple intrusion tactics can be used to circumvent detection and allow for covert access to the machines and in most cases, all the equipment and training an attacker would need to access the machines is conveniently available online (Tool 1991, TechRadar 2008). Secondly, the machines are often assumed to be tamper resistant due to the various security seals placed on the machines which is a pure fallacy as discussed earlier. Making matters worse, many of these locations are guarded by low wage workers who could easily be bribed to look the other way by an outsider and a corrupt election official could easily gain entrance to the

[26] In fact, average the "low" costs today are around $9,000 a year on transportation and $25,000 a year on storage (Norden, The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost 2006, 149).

facilities without question. As such, these machines are quite vulnerable to physical tampering while they are in storage.

These machines are actually even more vulnerable to physical access once they have been deployed to the various poll locations in the days prior to the election. In fact, in some instances machines have been deposited at polling places upwards of a week before the election (Appel, Security Seals on Voting Machines A Case Study 2011). As shown in Figure 11 below, the CalTech/MIT voting project reports that over 68% of Election Day votes in 2008 were done in very insecure schools, churches or community centers (Alvarez, Ansolabehere, et al. 2012, 31). As such the machines can be easily accessed in many cases without any concern for security guards, locks, cameras or any sort of detection.

Figure 11: Exposed Voting Machines
(Appel, Ginsburg, et al., The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine 2009, 3, Appel, Security Seals on Voting Machines A Case Study 2011)

Since the security is quite poor whether the machines are deployed or still in storage, the choice of when to physically access them depends on timing. When accessing the machines at polling locations, the attack must be carried out in the few days prior to the election which only provides a small time window to attack the machines. If it turns out that some late night meetings were occurring at the church or school, a non-ideal night may have to be chosen for attack due to the small time window. Fortunately for an attacker, the spread of early voting is increasing the amount of time the machines are exposed at polling locations. Even still, when machines are in storage an attacker can wait for weeks or months to find the perfect day to attack. This not only gives an attacker more flexibility but allows him or her to spend a lot of time studying the behaviors of the various workers and security guards who may be in the area allowing for an optimally covert intrusion. On the flip side however, when the machines are attacked weeks before the election, the attack code will be based on the political realities from weeks before the election and can't be updated later, which could lead to major issues in the attack. In fact, Gallup Polls showed that between the October 17th and November 4th polls for the 2012 election, Republican challenger Mitt Romney went from a 7 point advantage to only a 1 point advantage greatly changing the projected election outcome (Gallup 2012). This type of drastic difference would greatly affect the scale and style of attack needed. Therefore, attacking the deployed machines, while more risky in its time frame and preparation ability, would allow the attack code to be finer tuned and more accurate.

In either case once an attacker gains physical access to a machine he or she can easily load in the attack code by simply swapping out the firmware running the machine. In fact, in a detailed study Professor Andrew W. Appel of Princeton University showed how every single different type of security seal can be easily bypassed from adhesive tape to plastic straps to wire straps to combination locks (Appel, Security Seals on Voting Machines A Case Study 2011). Therefore, through use of a simple Torx security screwdriver (McDaniel, et al. 2007, 55), one can replace the PROM, or other internal flash memory chip, with one with firmware containing attack code. Once this malicious firmware is installed on the voting machines, the attacker has full control over their functionality. That all said, attacks on machines in storage or after deployment are focused on PCOS and DRE based systems as vote-by-mail systems use central count scanners which often remain at election headquarters.

DREs also provide one more opportunity to physically access the machines: Election Day itself. This is because only in DRE systems do voters get to interact privately with a voting machine. At first pass, the fact that voters have private access to DREs during voting does not seem to be a problem as the software is designed to prevent a voter in voting mode from being able to access any administrator functions and change the way the election is running. Unfortunately, most machines were designed quite poorly in ways that fully expose removable media slots to voters during voting as shown in Figure 12 below.

Figure 12: Exposed Removable Media Slots on DREs
(Feldman, Halderman and Felten 2007, 1, McDaniel, et al. 2007, 66)

As such voters are given the opportunity to insert custom removable media carrying attack code into the machine and launch attacks through the buffer overflows in the removable media reading code. And, as discussed earlier even if the interfaces were not for standard removable media the custom hardware can be emulated. In fact, in Figure 12 on the right one can see a security researcher demonstrating the Palm Pilot and magnet emulation of a PEB on an iVotronic. Furthermore, whether an attacker is using COTS hardware or an emulation of custom hardware, the hardware used is both incredibly small and commonplace. Therefore, not only can it easily be concealed in a pocket and brought into the voting booth, but even if voters were searched, such items should not arouse any suspicion. Even if a voter doesn't launch a new attack via custom removable media, a voter can still inflict a lot of damage on the voting system due to access to the poorly designed machine. For one, a voter could remove or break the devices which in many cases could lead to a loss in the votes from earlier in the day. An attacker could also simply unplug the VVPT cable which is often attached in an easily accessible location, as exemplified

by the iVotronic shown in Figure 13 below, and therefore remove the possibility of an audit. An attacker could also use his or her election day access to a DRE to perform a "cryptic knock," a pre-arranged type of voting operation such as tapping the corners of the screen in a specific order, in order to initialize the attack code on a machine and ensuring that the attack code could never be initialized except during voting hours. Therefore the poor design of and private voter access to the DRE invites a whole series of extra ways to launch attacks.

Figure 13: Exposed VVPT Connections
(McDaniel, et al. 2007, 46,72)

Unfortunately for an attacker, even if one was able to access each of the machines individually such attacks do not scale very well as each machine does not service that many voters. This number scales much differently depending on the type of system deployed. This occurs because DRE based systems require multiple DREs per precinct, while PCOS systems have only one scanner per precinct. In fact, common numbers reported for voters per DRE machines range from only 86 (Overton 2006, 44) to 300 voters (Alvarez and Hall, Electronic Elections 2008, 39). That said, attacking a PCOS system or a room full of DREs covering an entire precinct does not scale much better as it would only lead to an attack of on average 600 to 1450 votes[27]. Also, many of the scenarios described above require breaking into or accessing the machines at either the voting location or when they are all grouped together in a central warehouse. Therefore, the only difference between attacking a PCOS or DRE based system would be the amount of machines needed to be attacked at each location and as such a PCOS system is only easier to attack in the sense that significantly less time needs to be spent during the attack. That said, attacks on central count scanners could lead to attacks on an entire district which could be as high as the previous mentioned 2.2 million voters in Los Angeles Country and thus could scale very well.[28] Therefore, while individual attacks against machines appear to be quite easy to achieve covertly at a variety of time windows before or during the election, such attacks do not usually scale well enough to affect a national election without many accomplices working together to perform the attack.

[27] This is based off of the 606 voter average number in *The Machinery of Democracy: Protecting Elections in the Electronic World* which also states a 125 vote number for DREs. As such since this number is 2.4x smaller than the 300 number for DREs from *Electronic Elections*, I took the 606 number and scaled it up for the 1450 upper bound (Norden, Lazarus, et al. 2006, Alvarez and Hall, Electronic Elections 2008).
[28] Although again these scanners are cooped up in election headquarters.

Section 5.2: Attacking the EMS

"If the EMS is not kept secure we know of no practical method for ensuring the security of the polling place (Halderman, et al. 2008, 2)."

Ideally attacks against PCOS and DRE systems could also be scaled to the district level, like attacks against central count scanners. The first major place at which all of the deployed PCOS or DRE machines are all networked and could be exploited in such a way is the EMS. This occurs since all of the ballot definition files and resultant removable media are prepared, initialized and distributed from the EMS before the election and all of the removable media holding vote totals are connected back to the EMS to total the votes from the various machines following the election. Therefore, the big question is how to get the attack code onto the EMS and fortunately for an attacker, there are two ways in which this can be achieved.

The first way to get attack code onto the EMS is to outright attack the EMS. This can be done by breaking into election headquarters (where the EMS is supposed to be stored) and hacking into the machine and installing some attack code onto the machine. Since most EMSs run on standard COTS software such as Microsoft Windows, as explained earlier, getting attack code onto the machine and bypassing any basic security mechanisms on the computer should be relatively trivial as known flaws in the underlying COTS software can be used to attack the machine. In fact, Microsoft's Security Response Center's blog posting on the 10 Immutable Laws of Security states as law number three that, "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore (Microsoft 2012)." Therefore, the only mitigating factor in attacking the EMS in this way is gaining physical access to the EMS. As long as it is stored in election headquarters, it is relatively secure, although many town halls still possess relatively lax security and have been broken into in the past couple of years (McNeece 2009). Regardless, this attack vector also has the benefit of allowing the attacker to install his attack code in the days leading up to the election as the removable media is not usually primed for distribution until right before the election to allow for legal last minute changes.

If an attacker did not want to risk breaking into any buildings, and the district was using a DRE based system, he or she could still attack the EMS through an attack on a DRE in the previous election. As the EVEREST report explains:

"For example, a voter can compromise an iVotronic terminal [a DRE] through its PEB slot. The iVotronic, then, may be programmed to crease results media (at the end of the election day) that, in turn, corrupts the software of the central Unity system [the EMS]. The compromised Unity system, in turn, may be programmed to load corrupted firmware into all M100s [a PCOS] and iVotronics in the country when provisioning the subsequent election. At this point, every major component of the system is running compromised code, which originated with a single attacker with only voter access in a single precinct. Needless to say, such an attack represents a grave threat to the integrity of the elections of any jurisdiction to which this happens (McDaniel, et al. 2007, 57)."

This is especially powerful if a special election or primary election is held close to the date of the target election, but becomes less effective as the time between elections increases drastically as this would lead to an attack based on outdated information. For example, in Ohio in 2012 the closest election to the November 6th general election was the June 12th primary election (Office of the Secretary of State of

Ohio 2011). Fortunately for an attacker in 2012, the poll numbers from June 11th showed Obama leading by 1 point which was very similar to the final poll numbers that showed Romney leading by 1 point (Gallup 2012). However, in the 2008 election, Obama held a two point lead over McCain at the time of the primary and at the special election in between the primary and general election, but at the final poll he was leading by 11 points, greatly changing the calculations behind an attack (Gallup 2012, Office of the Secretary of State of Ohio 2007). Therefore, while this attack vector is much safer for an attacker and is raised as a major concern by security researchers, it may not be very useful in practice due to the major timing issues. Making matters worse for an attacker, some districts also re-set their EMSs in between elections by completely erasing the memory on the machines and as such wiping out the attack code (although a properly designed virus could survive a system wipe if the district used the same physical hardware, but that is also not a guarantee). In general this attack vector requires that the attack is distributed too far in advance to be particularly useful. However, with the assistance of an insider this attack vector becomes plausible. For example, an insider who has been charged with instructing the poll workers on how to perform their basic tests on the machines could potentially include a specific name which the poll workers need to use to test the write in candidate functionality. The spelling of this name could actually be an encoding of the instructions for the attack code (Norden, Lazarus, et al. 2006, 38). Of course this requires one to have unique insider access and thus this timing issue is still a major issue.

It is also important to note that attacking the EMS is not a panacea for scalability as one only gains access to an entire district's voting machines and voting district size varies greatly by state and within states. In fact, using Ohio as an example and basing data off of voter roll data updated January 27, 2013, wide variation in the size of voting districts can be observed in Ohio's voting districts which are broken up by county. The largest county, Cuyahoga County, representing greater Cleveland, had 928,907 registered voters, while the smallest county, Vinton County, representing a rural section of south central Ohio, had only 8,706 registered voters, less than 1% of the amount of voters in Cuyahoga County (Office of the Secretary of State of Ohio 2013). Making matters worse, the number of registered voters does not predict how many voters will actually vote in the election. For example while Cuyahoga and Vinton Counties had 66 and 67 percent voter turnout in the 2012 election, across the state voter turnout rates varied from a high of 77 percent in Delaware County to a low of 27 percent in Van Wert County (Exner 2012). Consequently, attacking an EMS can vary greatly in the number of voters affected, and in order to attack an entire state, in most cases many EMSs would have to be compromised. For example, Ohio alone has over 80 different counties each with their own individual EMS (Office of the Secretary of State of Ohio 2013).

However, this difference in sizes between districts can actually improve the scalability of attacking EMSs by allowing for a focused attack on key EMSs. By targeting only large voting districts or medium sized but highly partisan districts, election totals can be attacked in a scalable manner especially given the preponderance of large voting districts around major cities in the United States. For example, in Ohio, attacking only the five biggest counties would already capture over 40 percent of the potential electorate as is shown in Figure 14. Therefore, attacking the EMSs is a very good strategy for scaling up an attack on PCOS and DRE machines.

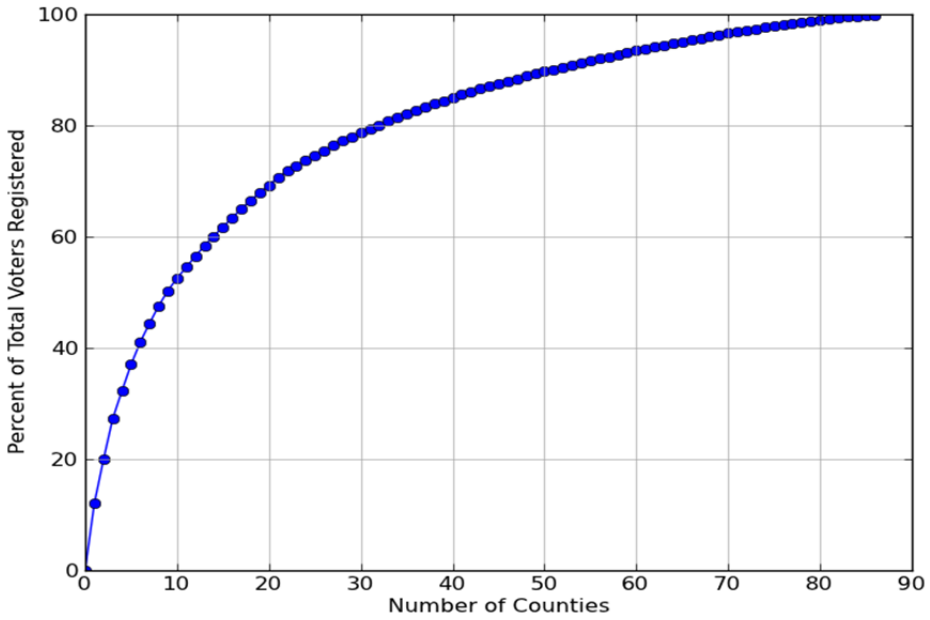

Figure 14: Percent of Total Voters in Ohio by Number of Counties
(Office of the Secretary of State of Ohio 2013)

Section 5.3: Wireless Access Attacks

"The same wireless, mobile technology that is liberating almost every aspect of our daily lives brings risks that few may have anticipated even as we marvel at our ability to organize our work, health, finances, travel and even home refrigerator temperatures from anywhere at anytime." –Pat Calhoun, Sr. Vice President and General Manager, Network Security, McAfee (Calhoun 2012)

While attacking the EMS can scale well, ideally an attacker would not need to enter the building in which the EMS or voting machines were stored and instead attack the machines remotely over the internet. Although voting machines normally are not attached to the internet, some machines were produced with wireless capabilities installed in them for potential future use. As such, it is possible to attack some of these machines via the internet. In fact, the Brennan Center for Justice noted that even if the wireless cards are disabled or turned off, software attacks can be designed to re-activate the wireless components on the voting machine (Norden, Lazarus, et al. 2006, 85). This means that any machine that has a wireless card installed in it can be accessed from the internet and attacked. This is why Virginia passed a law last year banning the purchasing of devices with wireless components, but fortunately for attackers, due to cost concerns, the law did not ban the use of already purchased machines with wireless components and other states with machines that have wireless components have either passed similar laws or no laws at all (Hickins 2012).

Attackers also have the benefit of years of hacker research into the art of breaking into wireless networks and accessing networked devices. In fact, there are entire websites dedicated to these arts whether it is through the use of online penetration suits such as the previously mentioned Metasploit or

through the use of WarDriving[29] to manually pinpoint and attack wireless networks (WarDriving.com 2012). Therefore, if the building in which the machines were located had wireless internet capabilities, an attacker could simply attack that building's internet connection and piggyback off of that connection to gain access to the voting machines and upload attack code. Given that many of these machines are often deployed in schools, community centers and churches, all places that often have wireless internet connections; this is a very likely scenario. Even if the buildings did not have wireless internet connections, since 94% of all Americans have internet access (Terry 2012) it is highly likely the building itself has an internet connection. Therefore an attacker could ahead of time install a wireless network adapter in the building in order to enable wireless access. This installation would be quite covert as it is highly unlikely that anyone would either notice this installation or complain about its existence given the ubiquity of wireless today. Even if that failed, the attacker could WarDrive by the building, pinpoint the machines with a strong antenna, and attack them in that manner. While this manual driving around does not scale as well, it would allow an attacker to attack an entire precinct at the same time without breaking into any buildings, so it still scales a lot better than physical attacks on individual machines. Also, an attacker could easily leave an antenna directed at the machines attached to a cell phone or other remote internet broadcasting device in a concealed location to allow for later remote access after the WarDrive was completed. With any of these methods in use an attacker could upload his attack on Election Day and update it as the day progressed on those machines giving him a huge advantage on accuracy over attacking an EMS. The question therefore becomes: how many machines are still deployed with wireless capabilities?

Verified Voting reports that there are three precinct based models and one central count scanner deployed around the United States that have wireless capabilities, the Sequoia Optech Insight(+) and ES&S DS200 PCOS machines, the AVS WINVote DRE and the AVS WINScan central count scanner. These machines service over 24 million voters in over 15 states and are used as standard polling place equipment, accessible polling place equipment, and central count scanners for vote-by-mail and absentee ballots. This leads to wireless enabled PCOS machines assigned to over 58% of registered voters in Arizona, 47% in Florida, 36% in Illinois, 28% in New York, 9% in California, 7% in Ohio, and 5% in Washington State and also leads to wireless enabled DREs assigned to over 16% of registered voters in Virginia (Verified Voting Foundation 2012). As long as the attack plan required a low level of WarDriving, and these wireless enabled machines are not taken out of service anytime soon, this attack vector can scale very well. Therefore, if an attacker wishes to attack the states mentioned above, the polling locations that use these wirelessly enabled devices should be carefully examined in order to see if such an attack could apply, and if so, this attack vector becomes quite compelling.

[29] WarDriving is the practice of driving around in a van with a strong wireless antenna and manually pinpointing wireless networks and then penetrating those networks to either gain information from the network or to leach off of the network and gain a free internet connection.

Section 5.4: Vendor Attacks

"I am committed to helping Ohio deliver its electoral votes to the president next year." – Walden O'Dell, Chief Executive Officer, Diebold Inc. 2004 (Krugman 2003)

While wireless and EMS based attacks can be quite powerful the hope for an attacker is that there is still an attack vector out there in which all of the machines are networked remotely in order to further increase the scalability and covertness of an attack. Fortunately for an attacker, there is one instance in which mass remote scalability occurs, on the rare occasions that the firmware on a machine is updated. This requires the machines to be attached to the internet for a remote update from the parent company and provides a golden opportunity to attack an entire class of voting machines. In these situations the machines are completely vulnerable as whatever firmware is delivered to the machines will become their firmware moving forward. Therefore, if an attacker could swap out the delivery with his own firmware which contained his attack code he could infect the machines. Even better, all types of machines need firmware updates from time to time and as such the attacker could use this to infect all machines around the country. The one main issue with this attack vector is timing as these firmware updates are rare and do not occur predictably.

The attacker can replace the firmware with his own version at three different occasions: while the firmware still resides on the company's servers before transit, while the file is in transit, and while the file is being downloaded by piggybacking on the internet connection and changing the source of the download to an infected copy. While the later methods would only involve attacking the target machines or internet packets, thus removing the need to carefully hack into the company's servers, they requires impeccable timing. Not only would the attacker need to have the attack code ready at the exact moment the download occurred, but the attacker would need to be monitoring all traffic to know when it occurred and be able to execute the attack in real time. While a running script might be able to initiate the attack, the exact IP addresses of the machines might not be fully known ahead of time and there might not be enough time for humans or scripts to figure out all the places to attack before the download window closed. On the other hand, while breaking into the corporate network is more difficult, it is probably feasible given the rash of corporate break-ins seen recently. Also once in the network an attacker could not only see the full source code and therefore explore the best ways to insert and obfuscate the attack code, but could also see internal communications and emails and therefore know exactly when the update was going to occur. This would allow the attacker to add his code to the source code, or even the binary file if he was skilled enough, after the source code had been thoroughly review by both internal and external reviewers and was cleared for deployment. Therefore, the attacker could avoid detection of his or her changes.

At the same time, if the attacker could gain the help of a coder working for the company this would make the attack even easier. In that case, the attacker would neither have to hack into the network, nor learn the code base to design the attack, but would simply instruct the employee on what the end result should be. This would also mean that if the attack code's introduction was logged in any manner it would appear at a quick glance as a legitimate edit by a legitimate employee. Furthermore, the employee would be more likely to be aware of all of the logging procedures and could therefore better protect the update from detection. Such an insider attack is also not unprecedented. In the early 1990s,

Ron Harris, a mid-level computer technician for Nevada's Gaming Control Board, managed to install attack code on dozens of video poker and slot machines and was therefore able to make a lot of money gambling with the odds wildly in his favor. He was even able to get completely away with it and only got caught years later when his hubris got the best of him and he had his accomplice attempt to take out a $100,000 jackpot winning on a Keno game (Norden, Lazarus, et al. 2006, 33). Insider attacks from voting machine company employees therefore must be seriously considered. Of course the difficulty with this is that the attacker must either find an accomplice or become an employee at the company itself. And since there are many companies and being employed at all of them would be impossible, it would in either case necessitate working and trusting with a handful of accomplices if one wanted to attack all machines in the country thus raising the chance of detection and the amount of people involved in the attack. In an extreme case, the attacker could potentially buy a whole company in order to gain control over the software. Given the sticker price of $5 million with which Diebold agreed to sell of its voting machine division to ES&S in 2009 (Zetter, Diebold Unloads Beleaguered Voting Machine Division 2009), and the over $35 million Sheldon Adelson personally spent in the 2012 election cycle, this actually does not actually appear to be out of the question (Cline 2012).[30] Either way, having an insider in the company greatly increases the effectiveness of this attack venue.

The firmware update attack vector, however, suffers from the fact that updates are not often done close to an election. While a crafty insider can greatly reduce this burden by "suddenly" noticing a critical flaw which requires an emergency update days before the election,[31] this type of attack also suffers from the same scaling issues as the EMS based attacks since there are multiple types of machines being voted on throughout the country and the percentage of voters using each machine varies wildly. In fact, as shown in Figure 15, while ES&S's AUTOMark and Diebold's AccuVote OS each service over 10% of the registered voting population, the final 10% of the registered voting population is served by 29 different types of machines. Similarly, as shown in Figure 16, while ES&S and Diebold each respectively service 29% and 21% of the registered voting population, the final 15% is serviced by 11 different vendors, or no vendors at all in the case of hand-counted ballots (Verified Voting Foundation 2012). Therefore, similar to the situation with the EMSs, this enables an attacker to attack substantial portions of the population by attacking only a few target models or vendors, but requires widespread attacks to attack the entire country.

In conclusion, this chapter shows that there are a variety of vectors from which attacks can be launched, that each has a variety of pros and cons, and that the main issue facing an attacker is the scalability of his or her attack. Therefore, the next logical question is given all of the attack vectors on both the system at large and the machines themselves, could someone actually combine all of the options and historic trends explored in this and the previous chapters and steal a presidential election? That is the question the next chapter seeks to answer.

[30] Along those lines one could also envision purchasing the company which produces the machines or at least buying off one of the suppliers. In this way an attacker could sneak wireless cards into the machines, install a malicious BIOS which would always notify the attacker if the firmware was updated or insert other malicious extras into the machines in order to allow for easier attacks.

[31] In fact, there was a controversy that broke right before the 2012 election when Ohio Secretary of State Jon Husted authorized ES&S to install "experimental" software in 39 counties (Levine 2012).

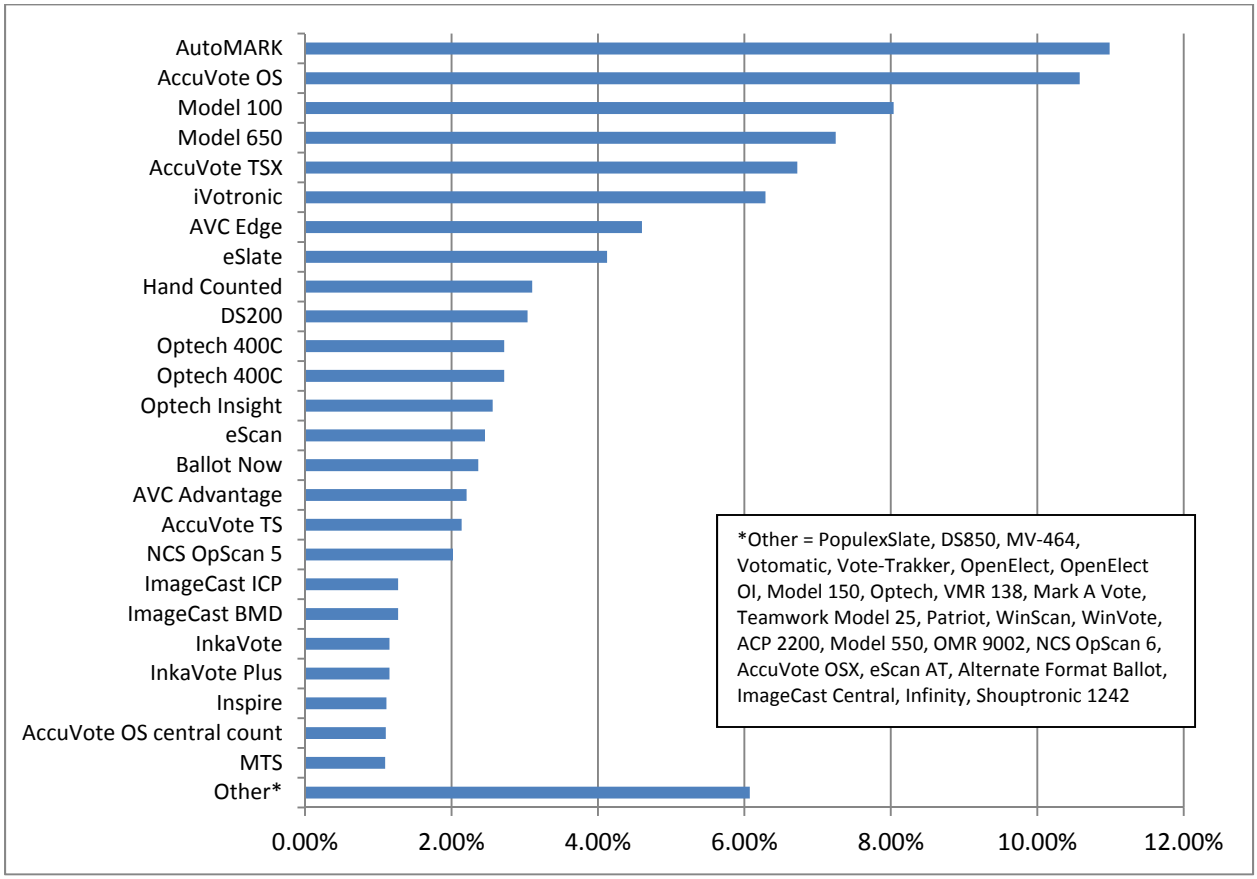

Figure 15: Percent of Total Voters per Machine
(Verified Voting Foundation 2012)

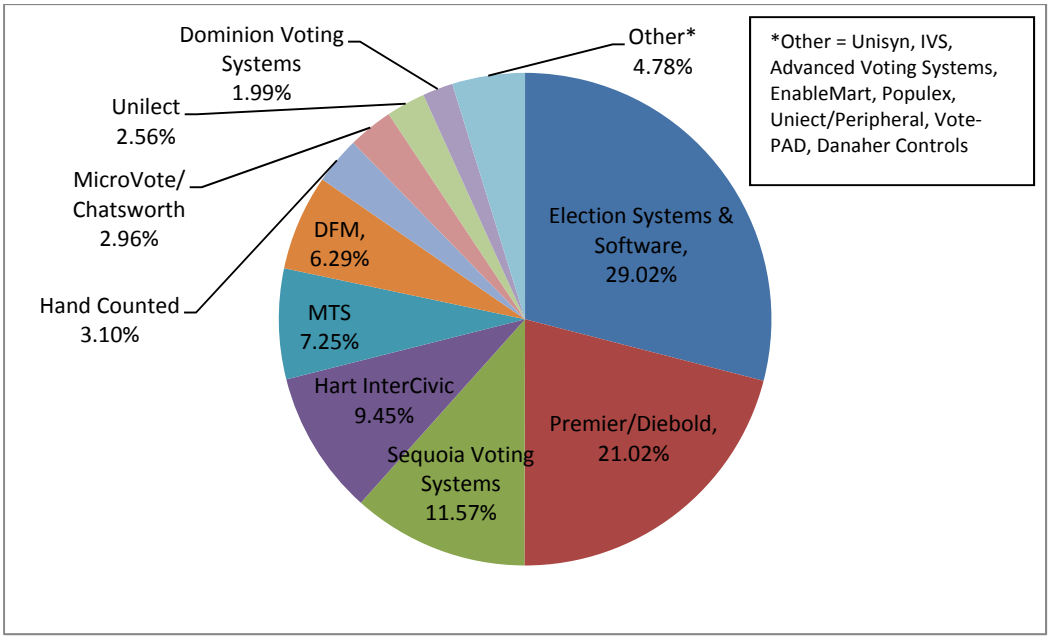

Figure 16: Percent of Total Voters per Vendor
(Verified Voting Foundation 2012)

Chapter 6: The Blueprint for 2012

"G. Robert Blakey, a former special prosecutor … [said that] from FBI wiretaps he had heard, 'enough votes were stolen – let me repeat that – stolen in Chicago to give Kennedy a sufficient margin that he carried the state of Illinois [and with it the entire election in 1960]' (Gumbel 2005, 167)."

Based off of the research in the previous chapters, I decided to assume the role of an attacker and begin an analysis of how I would have attacked the 2012 election. This will not only help me better understand where and when an attack can occur, but will also help me figure out how to prevent a future attack. My quest is to determine which combination of attacks will form the optimal attack on the 2012 election. The answer to that, of course, depends on the intents of the attack and the risk profile I am willing to assume in stealing the election. Therefore, the assumption made at the beginning of the paper must be revisited. With that in mind, it is time to step into the political reality that was May of 2012, 6 months to Election Day.

Section 6.1: Acquiring the Targets

"Choose your battles wisely. After all, life isn't measured by how many times you stood up to fight. It's not winning battles that makes you happy, but it's how many times you turned away and chose to look into a better direction. Life is too short to spend it on warring. Fight only the most, most, most important ones, let the rest go (C. 2013)."

The assumption stated in the beginning of the paper is that the intent of the attack is to covertly steal a presidential election. Furthermore as an attacker I only want to enact an attack that will succeed, or at least be projected to succeed, due to the large risk involved. Therefore, the attack scenarios and targets are quickly limited to attacking only four models of DRE machines, both with and without VVPT, in six of the swing states.

In order to ensure that the result from an attack will be deemed plausible by the population at large, only states in contention can be attacked. Therefore, the eleven swing states as defined by the pundits and polls in the late spring will be the focus of the attack. Without those states in play the challengers, former Governor Mitt Romney and Congressman Paul Ryan, have 191 electoral votes from their safe states and the incumbents, President Barack Obama and Vice President Joe Biden, have 201 electoral votes. The incumbents only need to capture 69 more electoral votes while the challengers need 79 more to reach the 270 electoral vote total needed for victory. As the swing states have a variety of different electoral values: Colorado – 9, Florida – 29, Iowa – 6, Michigan – 16, Nevada – 6, New Hampshire – 4, North Carolina – 15, Ohio – 18, Pennsylvania – 20, Virginia – 13 and Wisconsin – 10, a variety of different combinations of states can render either candidate the winner.

For further reassurance of lack of detection, I want to attempt to switch as few votes as necessary to win the election. Since the majority of these states either have automatic recount provision for close elections or policies in place that make it a low cost action for a candidate to request a recount in a close election (L. Norden, Issue Brief: Election 2012 Recounts 2012), attacks that do not pass an audit need to be cast aside in order to ensure that the attack is not detected during an audit or recount. Since I also want an attack that has a very high assurance a victory if implemented, I also do not want to undertake any attack vectors based on opt-in voter error. By opt-in voter error I mean attacks such as ballot design

attacks in which a voter has to make the mistake of voting twice to have the attack be a success. This is contrasted with opt-out voter error such as a presentation attack in which a voter only has to only not notice the error already made by the attack.

Given these criteria, attacks against PCOS and vote-by-mail based are ruled out as any vote changing attack is voided due to the built in paper trail and more subtle attacks such as turning off over-vote protection or stealing the paper trails either fall under the opt-in voter error category or are inherently risky, something I am trying to avoid. DREs on the other hand, with or without VVPT, still provide many opportunities for attack, and fortunately for my attack, many of the swing states use DREs as at least part of their voting system as shown below in Figure 17.

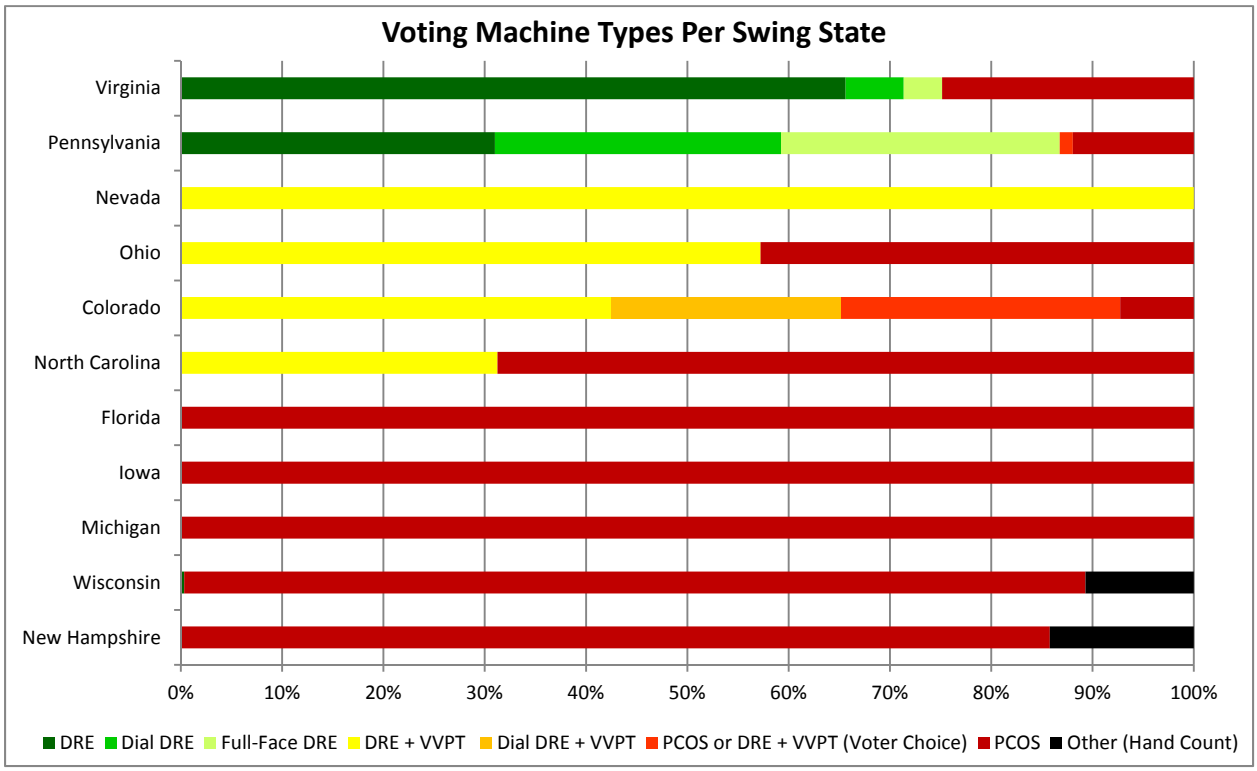

Figure 17: Voting Machine Types per Swing State
(Verified Voting Foundation 2012, Elliott 2012, Government Accountability Board: State of Wisconsin 2010, Government Accountability Board: State of Wisconsin 2012)

Figure 17 shows that the only states that I will consider attacking are Colorado, Nevada, North Carolina, Ohio, Pennsylvania and Virginia which conveniently sum to 81 electoral votes; just enough ensure victory for either Romney/Ryan or Obama/Biden. Since Obama/Biden ended up winning the 2012 election, for the rest of the theoretical attack, I will assume that I am attempting to steal the election for Romney/Ryan as that will lead to more interesting conclusions on whether an election can be won. Therefore, for a Romney/Ryan win all six states must be won.[32]

[32] This of course assumes that that all other swing states are lost. While not necessarily an accurate assumption, this is an assumption which a cautious attacker must make when designing an attack.

The next logical step in the attack is to determine which models of DREs are being used in those six states. This is important for two reasons. To begin with, I do not have the resources to develop attack code against every kind of voting machine used in America today. Secondly, if one company's machines are used in an overwhelming proportion then the best scaling attack vector is to attack through that company as it would represent a single point of failure nationwide. In running this analysis, for simplicity sake, I assume that all votes in voter choice districts are made on PCOS machines. This is not actually a very large assumption, as in fact many voter choice counties are moving to vote-by-mail systems/PCOS systems and only using the DREs for visually impaired voters ensuring that very few votes will be cast on the DREs (Liss 2012). With the voter choice districts removed from the analysis, the distribution of voting machines across those six states by percentage of registered voters is shown below in Figure 18. Unfortunately for the attack, it turns out that no single machine or company dominates the market in these six states. In fact, only AVC produces two machines used in the states and the most widely used machine, the ES&S iVotronic, is only used by just over 18% of the population.

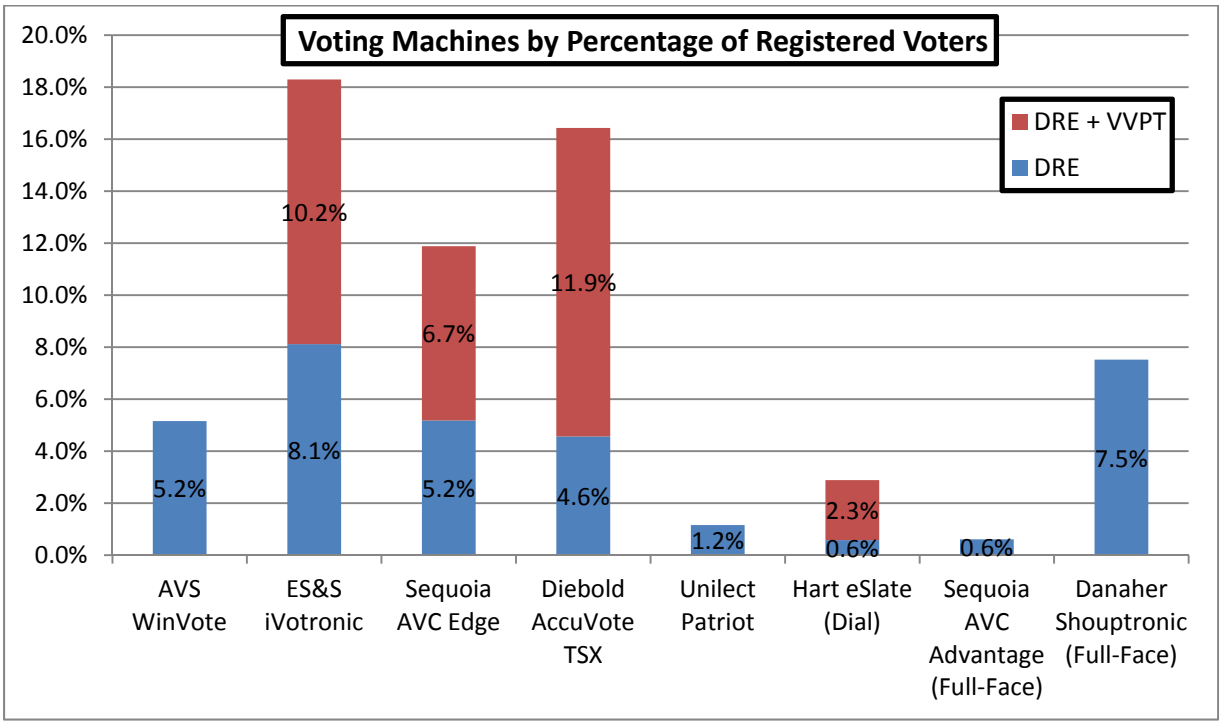

Figure 18: Voting Machines per Percentage of Registered Voters
(Verified Voting Foundation 2012)

Given that there is no immediately obvious scaling opportunity by using only one type of machine, the next step is to figure out exactly which models provide the best scaling opportunities. If it turns out that while 18% of voters are using iVotronics, that they are only being used in 5% of districts, then attacking the iVotronics provides a good scaling opportunity, but if they are being used in 30% of districts, that is not the case. The results are lukewarm as most machines are voted on by roughly the same percentage of voters as the percentage of counties in which they are deployed, especially amongst the biggest players. This is summarized in Figure 19. That said amongst the more niche players in the marker, the Shouptronic scales wonderfully while the eSlate scales terribly.

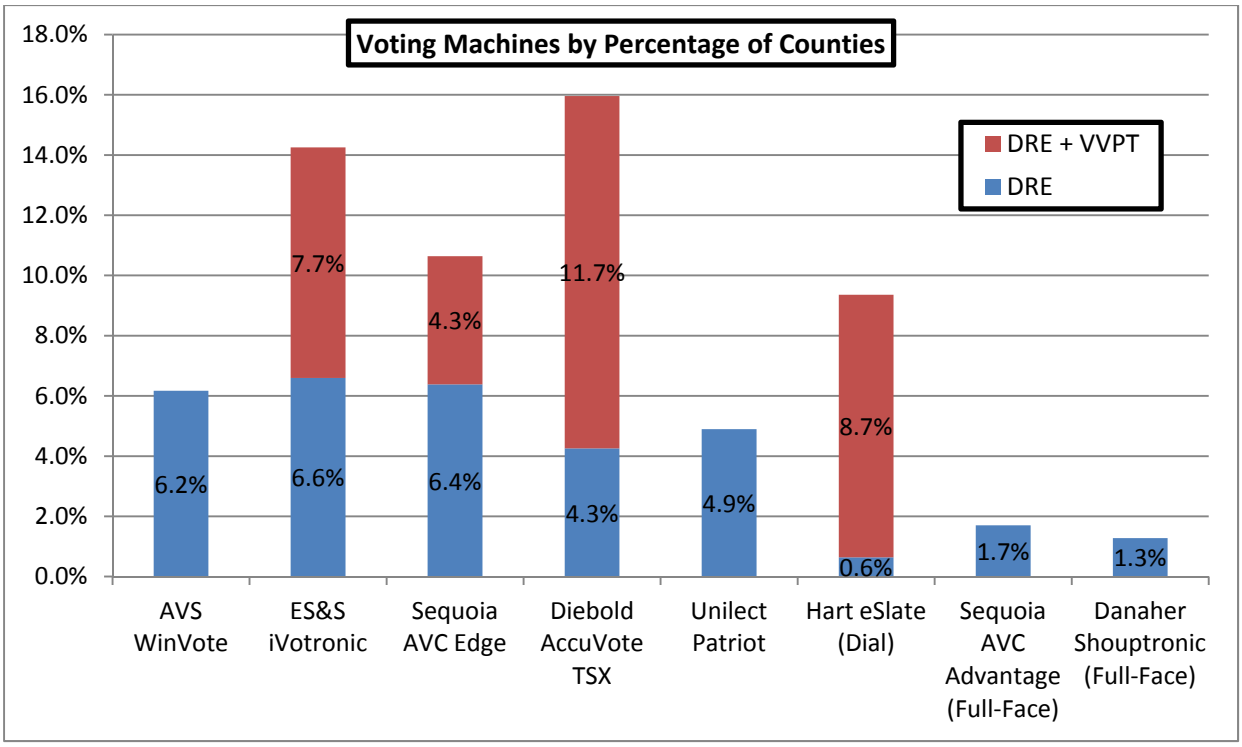

Figure 19: Voting Machines per Percentage of Counties
(Verified Voting Foundation 2012)

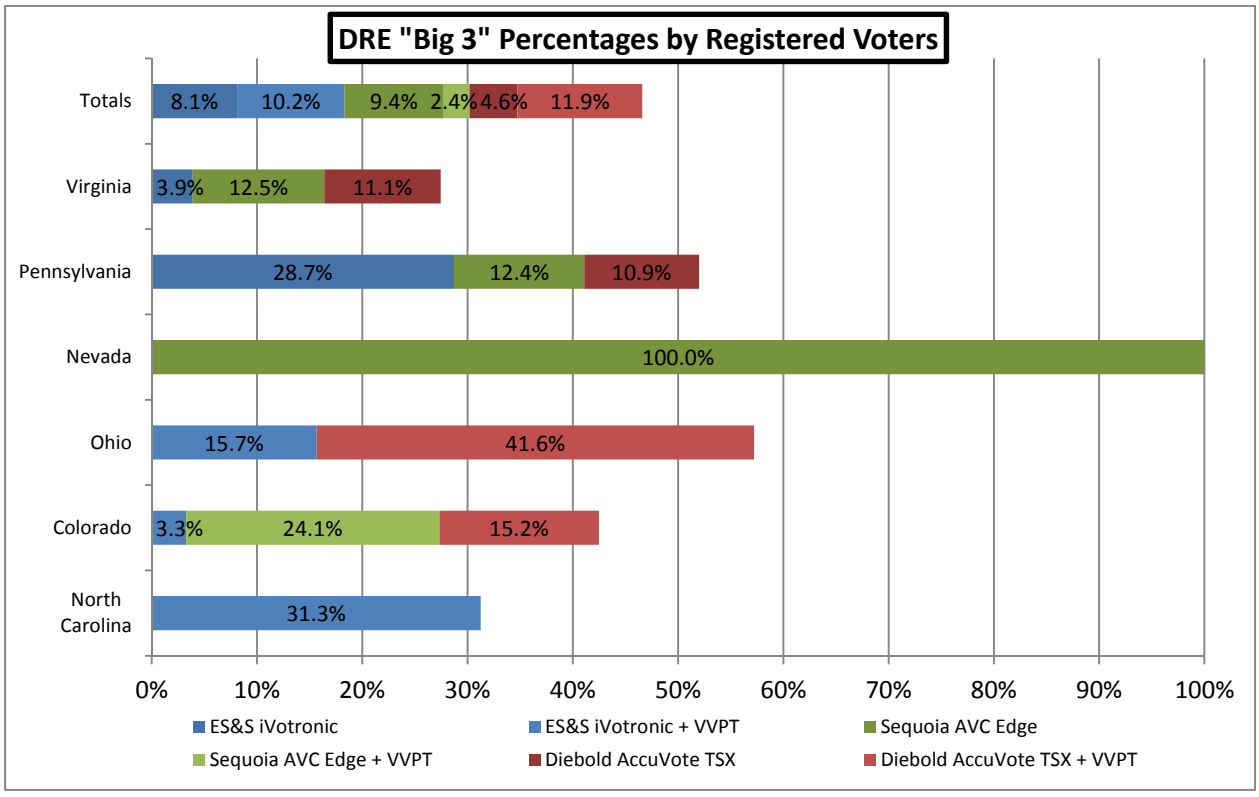

Figure 20: DRE "Big 3" Percentages in Key States
(Verified Voting Foundation 2012)

The iVotronic, AVC Edge, and AccuVote TSX, the three most widely used models, capture 46.6% of registered voters in those six states, providing enough scalability to enact a covert attack, my next step is to focus in on attacking those models. However, before settling in on those choices I first need to examine their usage at an individual state level as there is a chance that the high aggregate percentage might not hold up across all of the states. This data is summarized in Figure 20 and is quite promising as it is possible to capture 100% of registered voters in Nevada, over 50% in Pennsylvania and Ohio, and over 40% in Colorado. However, it is only possible to capture 31% of voters in North Carolina and 27% in Virginia. In North Carolina, only 31% of the state votes on DREs so no improvement is possible. However, almost 75% of Virginia is voting on DREs, making the 27% number unacceptable. Luckily, it turns out that 33.2% of the state is voting on the AVS WinVote (and is the only state voting on that machine), which is one of the machines mentioned earlier to have wireless capabilities. Therefore, expanding the target machine list to four machines by including the WinVote raises Virginia from 27% of registered voters to over 60% providing the scalability I desire.

The reason it is very important to try to keep the rates as high as possible is that not all voters will turn out to vote and others will vote via absentee ballots, which suffer the same problems with attack as PCOS machines. Therefore moving ahead in order to determine which voting patterns to study in each state, it is crucial to first determine which attacks and attack vectors should be considered.

Section 6.2: Selecting the Attack

"You must choose, but choose wisely. As the true grail will bring you life, the false grail will take it from you (Lucas 2013)."

Analyzing the various attack vectors and attack plans presented in chapters 3-5 in light of the assumptions made in the last section leads to a strict narrowing of the available attacks to essentially only the X% and presentation attacks through the EMSs as only these attacks and attack vector provide the stealth, assurances, and scalability needed to steal a presidential election.

Given my earlier assumptions and conclusions so far, attacks that do not have guaranteed numeric support[33] or attacks that result in the paper and electronic totals differing will not be considered. Along those lines, the fleeing voter attack, while extremely attractive in nature, is not supported by any available data and as such will not be considered.[34] I also quickly eliminate the simple P + - P = 0 attack as it requires accurate projections of the exact number of voters on each machine, which is almost impossible to implement programmatically especially if the attack code is distributed in a scalable manner. This eliminates every attack except the X% attack, its adaptation for VVPTs, the presentation attack, and the provisional voter attack. Figure 21 shows that the rate the provisional voter rate has been declining since the 2006 election is now pretty much irrelevant in Colorado, North Carolina, Ohio and Virginia, especially if the downward trend continues. It is also irrelevant in Nevada as the trend

[33] And while a victory cannot be guaranteed as polls are not 100% accurate, being able to guarantee a certain amount of the vote will be stolen is highly desirable for an attack. In that way an attacker can confidently conclude that if their candidate was to perform up to par or better in the election, then he or she would win.

[34] While I previously noted a theoretic rate of error of 6% and in another lab study with a very small sample size this voter error did occur (Greene 2008, 40-45), there is no data on statewide fleeing voter rates and as such no data upon which to guarantee effectiveness of an attack. Therefore, it must be ignored.

indicates that the provisional voter rate is incredibly low during presidential election years. However, it can be considered in Pennsylvania. Therefore, the attack plan will call for presentation attacks in all VVPT states and the X% attacks in all non-VVPT states besides Pennsylvania which can also be attack via the provisional voter attack.

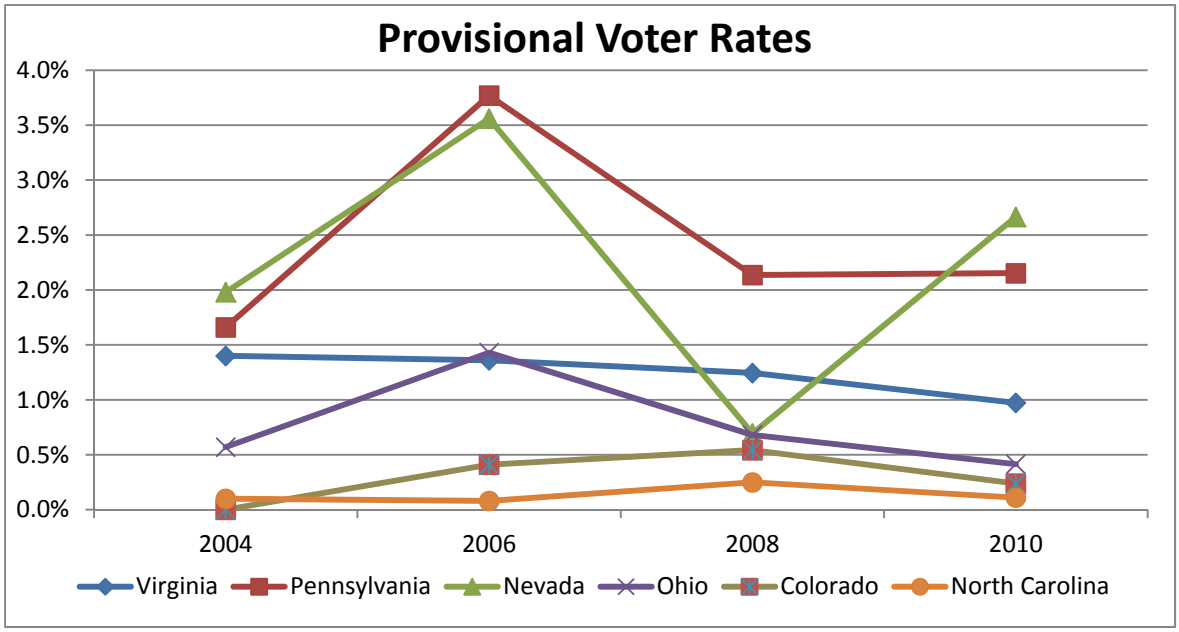

Figure 21: Provisional Voter Rates in Key States
(U.S. Election Assistance Commission 2011, U.S. Election Assistance Commission 2009, U.S. Election Assistance Commission 2007, U.S. Election Assistance Commission 2005)

Given that the presentation attack will be a very important attack and given that it has the aforementioned 3% notice of the attack rate, which I choose to scale up to 5% given the high profile nature of the presidential election and to provide some safety in the attack projections, it is important to consider how many of the voters who notice the attack will report the error and how often a poll worker would actually consider the report an issue. I believe that if the voter is able to correctly vote the second time around, not many people will complain about the error itself although they might complain about the buggy voting machines. That said following a worst case scenario, I have to assume that everyone will complain. It is therefore important to determine after how many complaints will a poll worker raise an alarm? Given the ubiquity of errors with the voting machines in the past, including over 18 separate counts of vote flipping across 6 counties that eventually got reported to the state (which of course excludes all of the people who had issues but chose not to complain) in West Virginia in 2008 alone (Goodman, Mulder and Smith 2012), and the amount of general confusion and errors made on Election Day by voters, the bar is relatively high. I am therefore going to assume that if each machine has only 1 or 2 reported errors in a day, and the machines are always able to fix themselves on a second try, no alarms will be raised during the election. After the election is over, and the reports are cataloged, one may notice the vast amount of VVPT errors and investigate. However, at that point the code will have already deleted off of the machines ensuring that the attack will be safe from detection.

Therefore, I need to ensure that the projected amount of noticed attacks on each machine is at most 1 or 2 attacks. Given that at most 300 people ever vote on a DRE, the noticing rate will increase linearly with the percent of voters attacked as N = 0.15P. That is, for each percentage of voters attacked (P) the number of projected attacks noticed (N) increases by 0.15. Therefore, attacking up to 13.33% of voters can be done without having more than 2 attacks noticed. Whether in a presentation or X% attack I also want to be careful to not to shift too large of a percentage of the vote in one district, otherwise the results will appear quite suspicious. Following the assumptions made by the Brennan Center for Justice, I need to make sure to only shift 15% of the votes in a given precinct, only 10% of the votes in a given district, and only 5% of votes in a given state (Norden, Lazarus, et al. 2006). Therefore, in the end, I can attack up to 10% of votes in a given voting district in order to shift 5% of the votes in a state.

I finally need to look at an overview of the ways to get the attack code on the various machines. As explored earlier, attacking the machines one by one would not scale well and thus is out of the question. Furthermore, with over 300 precincts in one of the four congressional districts of the largest county in Nevada alone (Clark County Nevada 2013), attacking the machines once they are deployed is untenable. And, given the assumption of 300 voters per DRE, this translates into over 2,000 DREs in usage in that same county. Therefore, even if all of those machines were stored in one location, which is highly unlikely, over 2,000 pieces of physical hardware would have to be tampered with in order to attack the machines in storage, rendering that attack vector untenable as well. Given the unpredictability of the timing of software updates, attacking through the voting machine distributers is out of the question as well. This is highly unfortunate due to the scalability of only attacking four distinct systems that could also be attacked over the internet through the voting machine companies' servers.[35] Therefore, the only attack vectors remaining are attacking through the EMS or via wireless access.

Since AVS WinVote wirelessly enabled DRE is one of the machines I am targeting in Virginia, the wireless access attack vector must also be explored. Unfortunately, given that it is not clear that I can force a machine to turn on via the wireless components, I will only be able to attack the machines wirelessly when they are turned on for testing purposes, which occurs sporadically and unpredictably like the timing for software updates, or once they are deployment and installed on Election Day (or the early voting days). Therefore, since the only time the machines would be realistically accessible via this attack vector is on Election Day itself and given that hundreds of precincts with unpredictable internet connectivity would have to be relied on as WarDriving would not scale without the use of many accomplices, this attack vector does not scale very well in practice. If I had an extended amount of time to canvas each precinct this could still be possible but at this time seems unlikely to be helpful.

Therefore, I am left with only one attack vector, attacking through the EMS. Unfortunately, in order to assume worst case scenarios, I have to assume that the EMSs are cleared between the primary and general election ensuring that the EMSs need to be directly attacked. Also while becoming an insider may be easier than expected as there were over 770,000 election officials and poll workers during the 2010 election (Alvarez, Ansolabehere, et al. 2012, 31), most of these insiders worked the polls in a precinct and did not have accesses to their district's EMS. As such only through bribery of a key election

[35] That said I would still attempt to gain access to the servers of the four companies in order to check their email traffic to see if a software update was going to happen in one of the key states.

official can I expect gain insider access to an EMS; a tactic that I believe is too dangerous and unreliable. I am also going to assume that no voting district was foolish enough to install their EMS on a computer that was either wired into the county intranet (thus accessible from the internet via a privilege escalation attack on the county servers), or had a working wireless card attached to it. Therefore, I will need to break into each election headquarters to access the EMSs in order to deploy my X% and presentation attacks (and provisional voter attack in Pennsylvania).

Section 6.3: Tracking the Targets

"The big secret to winning elections is to get more votes than your opponent." – Jesse Helms (Helms 2013)

The next step in the planning the attack is to focus in on the voting patterns in the six states in order to further explore the ease of attack on each state based on the true number of voters voting in the precincts, the size and number of districts in each state, and the poll data from each state. In the end the states show a wide variance in their return on investment from an attack, but an ordering is found.

Liberal use of absentee balloting is a major impediment to precinct voting rates. Fortunately, most of the states slated for attack do not show a significant loss of scalability form absentee balloting except Colorado which is quite worrisome as shown in Figure 22. That said, even in the other states, while these trends for the state overall may be manageable, certain districts may have very high absentee voter rates and turnout rates for voters can also vary widely by district. Therefore, all of these numbers need to be adjusted for in the overall analysis.

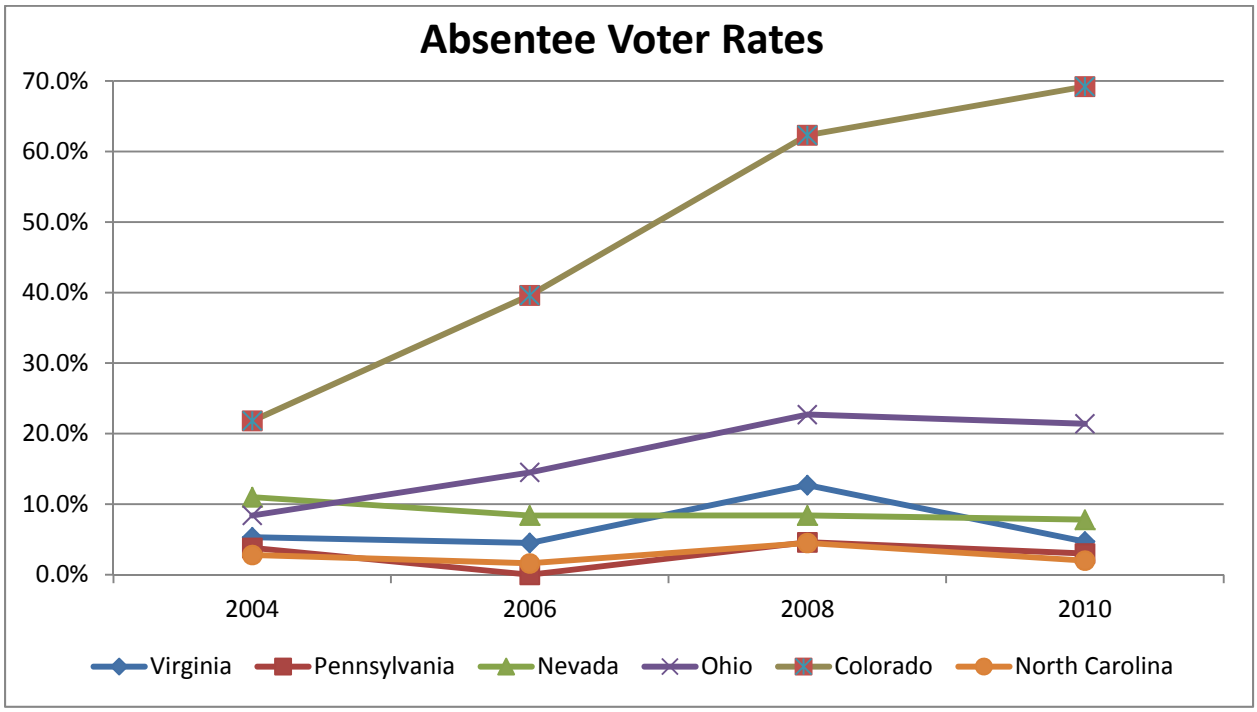

Figure 22: Absentee Voter Rates in Key States
(U.S. Election Assistance Commission 2011, U.S. Election Assistance Commission 2009, U.S. Election Assistance Commission 2007, U.S. Election Assistance Commission 2005)

The data driving this analysis comes from the 2010 election for absentee, provisional and early voting rates. In order to assume worst case scenarios for the attack, early and provisional rates are floored at 2010 levels whereas absentee counts are given a 5% overall bump from 2010 numbers which is not only consistent with the overall trend but also with the presidential election bump seen in the data (U.S. Election Assistance Commission 2011). The data also leverages voter turnout rates from the 2008 election as presidential elections tend to have significantly increased turnout from midterm elections. However, due to the record turnout in the 2008 election, the numbers are adjusted down by 5% of their respective values (Virginia State Board of Electors 2009, SOS Software 2010, Office of the Secretary of State of Ohio 2009, Office of the Secretary of State of Nevada 2009, United States Department of Commerce 2013, U.S. Election Assistance Commission 2009). Using this data one can project how many actual votes will be made on the machines in each district in each state. From this data, one can then calculate what percentage of the vote would need to be shifted in each district, based on the number of districts attacked in a given state, to shift 1% of each state's overall vote as shown in Figure 23.

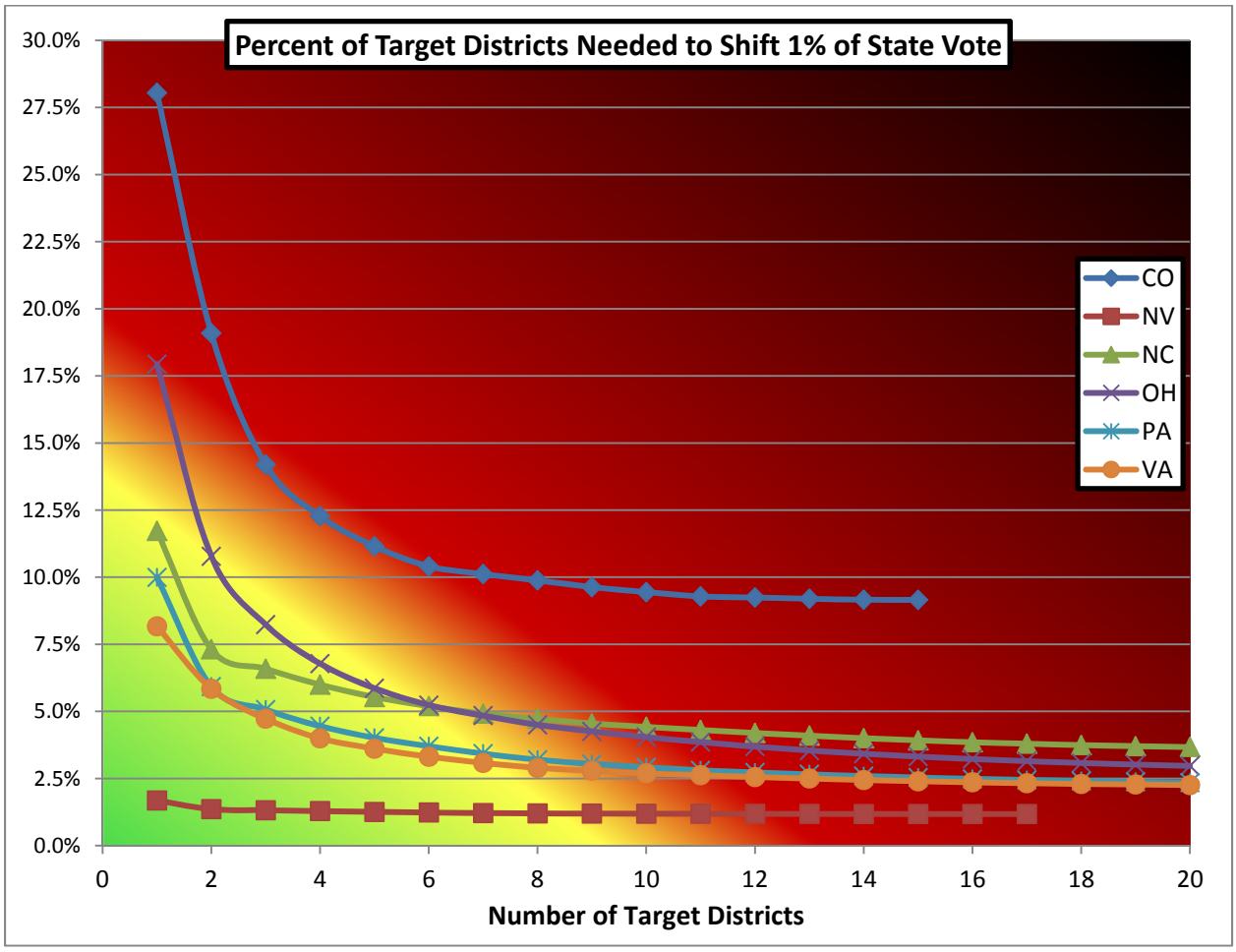

Figure 23: Attack Percentages per State to Shift 1% of the Vote
(Virginia State Board of Electors 2009, SOS Software 2010, Office of the Secretary of State of Ohio 2009, Office of the Secretary of State of Nevada 2009, United States Department of Commerce 2013, U.S. Election Assistance Commission 2009, U.S. Election Assistance Commission 2011).

This data shows wide variation in the ease of attack. While Nevada is in the green zone, as one can only attack 1 district and only have to switch less than 2.5% of the vote in that district, Colorado is in the red zone as at best one could attack 4 districts while shifting around 12.5% of the vote in those districts. Therefore, the next step is to combine this data with the poll data shown in Figure 24 and rank the states based on their return on investment due to their ease and likelihood of an effective attack.

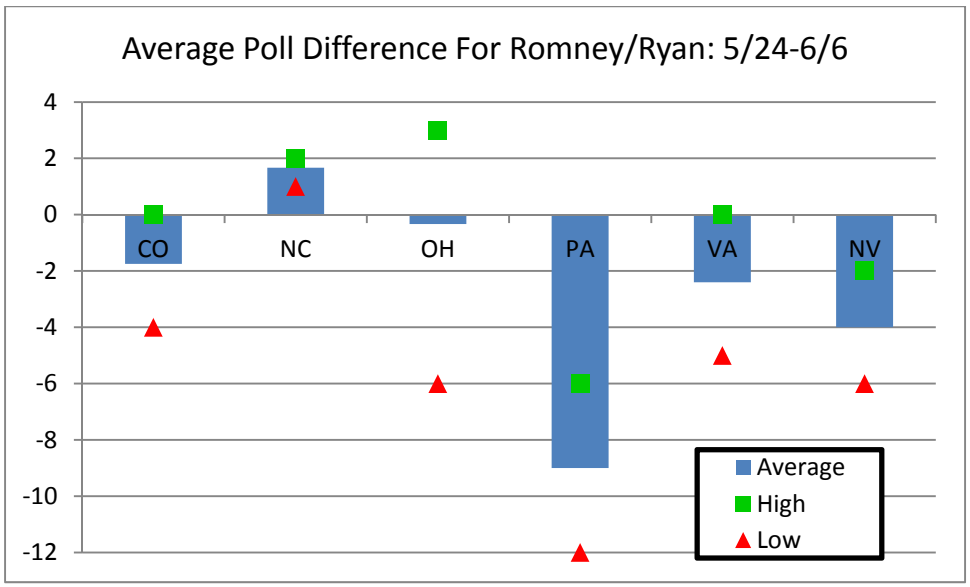

Figure 24: Late May to Early June Polls
(Elliott 2012)

From the poll data North Carolina can be seen to be in my favor and as such can be put on a back burner for the time being. At the same time, Pennsylvania is currently a lost cause and should also be ignored for now. The other states are very much in play and even though Nevada is the most pessimistic case left, it is the easiest to attack so is definitely a priority. My assumption of return on investment order is therefore as follows: Nevada, Virginia, Ohio, Colorado, Pennsylvania, and finally, North Carolina.

Section 6.4: Locking in on the Targets

"Auf wiedersehen. Bullseye (Tarantino 2013)."

It is now time to move to a state by state exploration of the voting districts and the appropriate ways to finalize the attacks on each state. In each analysis I consider the specific amount of districts to attack using X% or presentation attacks (and a provisional voter attack in Pennsylvania) deployed via the EMS onto the ES&S iVotronic, the Diebold Accuvote TSX, the Sequoia AVC Edge and the AVS WinVote. While each state is a unique target and there is a wide variance in the number of EMSs that need to be attacked and the percentage of votes that need to be shifted per district, parallels can be drawn between many of the states and well defined attack plans can be formed for each state.

Nevada: While Nevada is the first state targeted, that is not due to lax security measures in the state but simply due to its geography and voter demographics. Nevada actually does a fairly good job at protecting itself against attacks. The state's 17 counties all use the Sequoia Voting Systems' AVC Edge

Touch Screen DRE with a VVPT and the state has a post-election audit in place to reconcile the paper and electronic vote tallies. While the state does not mandate a full hand counted audit and allows for some of the audit to be done electronically, the state has never had less than a 100% audit match and therefore any deviation would be fully investigated (Goodman, Mulder and Smith 2012). Nevada, while not having an automatic threshold based recount does allow for candidates to initiate one as long as they put down a deposit for the cost of the recount in case it is unsuccessful. In a presidential election, with billions spent on adds, this would only be a minor inconvenience and as such a recount could easily be initiated. By all accounts the state is doing exactly what it needs to do to secure itself.

However, Nevada is still a prime target for two reasons. For one, Nevada has 87% of its population located in two voting districts: Washoe County, greater Reno, and Clark County, greater Las Vegas. As such, the scaling opportunities are incredibly tantalizing for an attacker. The second reason is that Nevada is a swing state whose voters chose to vote in high numbers at the actual polling locations. Therefore, not only do the attacks scale well theoretically but they also scale well in practice. Given that Nevada uses all machines with VVPT installed, the only viable attack profile is the presentation attack. Furthermore, since 2 counties cover 87% of the registered voter population and Clark County on its own covers 69% of registered voters, only those two counties need to be attacked. The focus on these two counties is heightened by the fact that they are the only counties in the state that voted for Obama/Biden in the 2008 election (New York Times 2008). Therefore, taking those counties, or even gaining enough ground in them, would swing the overall state. Since the state of Nevada had Romney/Ryan polling down around 4 points, my attack is designed to switch 4% of the vote. By attacking only those two counties, in order to switch 4% of the overall state vote, I need to switch just less than 5.5% of the vote. Adjusting for the 5% notification rate, I need to attack just less than 5.75% of the vote resulting in a projected error recognition rate of only 0.86 errors per machine, well within the bounds set in the previous section. Therefore, the attack plan would be to attack the EMSs of Clark and Washoe Counties outright to install a presentation attack designed to shift 5.75% of the vote by physically accessing election headquarters in the county seats.

Virginia: Virginia on the other hand is targeted due to its ease of attack. In the report "Counting Votes 2012: A State by State Look at Voting Technology Preparedness," Virginia received an inadequate on both paper trails and post-election audits. Over 75% of the state votes on DREs without a VVPT and over 44% of those DREs are equipped with wireless technology, making audits impossible and attacks easy (Verified Voting Foundation 2012, Goodman, Mulder and Smith 2012). This is only augmented by the fact that Obama/Biden was leading by just under two and a half points at the initial time window. However, Virginia is not the first on the list of states to attack as it does not scale nearly as well as Nevada. This occurs because while 75% of the population votes on DREs, no one district makes up a large portion of the population. In fact, the largest county with DREs, Fairfax County, only represents just over 12% of the overall population, nowhere close to the 69% of Nevada living in Clark County. However, the four largest counties with DREs encompass 25% of the overall projected voting population. As such an attack to gain back the 2.4% of the overall vote only requires switching 9.5% of the vote in each of those 4 counties. Since there are no VVTPs in use, my attack plan deos not have to worry about the 5% recognition rate. Therefore, an X% attack designed to shift 9.5% of the vote can be deployed on the EMSs of Fairfax, Prince William, Henrico, and Virginia Beach counties. As a final note,

these four counties were also Obama/Biden strongholds with an average margin of victor of over 10 points in the 2008 election making them prime targets (New York Times 2008).

Ohio: Ohio is greatly improving its election security. On February 24, 2012, the Ohio Secretary of State issued Permanent Directive 2012-12, requiring audits on even-numbered years and following presidential primary elections (Goodman, Mulder and Smith 2012). The state also only utilizes PCOS machines and DREs with VVPT, which ensure that recounts and audits are possible across the state. Furthermore, Ohio is not a panacea for scalability with its largest DRE county only covering 5.5% of the overall state vote. However, Ohio is the swing state polling dead even. As such it is an important target as moving a very small percentage of the vote could result in changing the overall state vote. Since less than 1% of the vote is needed to swing the election, one can attack only 3 counties and only have to shift, accounting for the 5% loss from VVPT notifications, 8.75% of the vote in those three counties to gain 1% of the statewide vote while only registering 1.3 projected discoveries of the attack per machine. Both numbers are well within the bounds previously discussed , and with those three counties voting for Obama/Biden 64.5%, 59% and 51.8% respectively in 2008 (New York Times 2008), the plan is to attack the EMSs of Franklin, Montgomery and Lucas Counties with an 8.75% presentation attack.

Colorado: At first glance Colorado appears to be in a similar position as Ohio. The state uses a mix of PCOS and DREs with VVPT and its largest county with DREs encompasses 12.5% of registered voters. Colorado has also been implementing various auditing schemes over the past few years in order to increase the security of its elections. Finally, Colorado was polling 1.75% down. However, what makes Colorado a lot different from Ohio and much more difficult to attack is the fact that Colorado has very liberal absentee voter laws which has resulted in roughly 60% of the state voting by absentee ballots as noted in the previous section. Therefore, even by attacking 6 counties, after adjusting for the 5% recognition rate, is necessary to switch 11% of the vote in each county (resulting in a 1.64 attack recognition rate) to change just 1% of the overall state vote. Therefore, the polls need to move more in Romney/Ryan's favor in order for the attack to be successful. Furthermore, since these 6 counties voted, 75%, 61%, 55%, 54%, 44%, and 34% for Obama/Biden in 2008 (New York Times 2008), moving 11% of the electorate would mean attacking almost 1 in 6 Obama/Biden voters in some counties greatly increasing the chance of detection. Thus while Colorado is a risky state to attack, since the polls only need to move by 1 point in order for the attack to be successful, and all of the attacks parameters are close to normal bounds, this attack can still be effective. Therefore, the EMSs of Denver, Arapahoe, Larimer, Weld, Mesa and Lake Counties would need to be physically accessed to install an 11% vote shifting presentation attack.

Pennsylvania: Pennsylvania also appears to be a much more attractive target than it actually is. Like Virginia, 81% Pennsylvania votes on DREs without VVPTs making an audit or recount nearly impossible. Pennsylvania also scales similarly to Virginia with 6 counties encompassing around 27% of the total voter population. The problem with Pennsylvania is the polls, which are 6 points down. Furthermore attacking those 6 counties requires shifting 11.1% of the vote in each country to achieve only a 3% shift in the overall state's election results. With an 11.2% attack in each county, to shift 3.5% of the vote requires attacking 8 counties and to shift 4% requires attacking 11 counties. Therefore, the 6 point margin cannot be defeated. Expanding to so many districts also ensures that some attacked districts will not have

primarily voted for Obama/Biden in the 2008 election as while the first 8 voted 60, 59, 57, 57, 55, 54, 43, and 41 percent for Obama/Biden in 2008, the final 3 voted on at rates of 48, 47, and 35 percent. Thus, the most attractive attack plan is to attack the first 8 districts for a 3.5% shift and hope that the polls move 2-3% in the next few months. Again, the attack needs to be deployed via physically accessing the EMSs in the various counties.

Pennsylvania also provides an additional attack vector through its relatively high rate of provisional voters, which can help shift even more of the vote. Figure 21 already established that a 2% provisional vote rate is to be expected in the state. To avoid detection, I would not want to shift all 100% of provisional votes to be votes for Obama/Biden but instead ensure that the project 54% of Obama/Biden votes would be shifted to 80%. As such, Obama/Biden provisional votes would be thrown out at a much higher rate than would occur naturally. This would result in a shift of a quarter of a percent of the vote,[36] increasing the 3.5% attack against the state of Pennsylvania to 3.75%.

North Carolina: Finally, I would reach North Carolina. Unfortunately, attacks again do not scale particularly well in North Carolina as only 31% of the state votes on DREs and the largest county using DREs only covers 8% of the state. North Carolina also uses all DREs with VVPT and has a mandatory audit law (Goodman, Mulder and Smith 2012). However, over 20% of the electorate can be attack through targeting only 7 counties. What makes North Carolina fall on the bottom of this list is, like Pennsylvania, the polls. Except in this case, the Romney/Ryan ticket is polling up one and two thirds points, meaning that an attack is likely unnecessary and attacking the state could cause more harm than good given the chance of detection. That said I still want to develop an attack plan in case the polls shifted out of Romney/Ryan's favor. Therefore, I want to plan an attack to move only 1% of the vote which can be done by attacking only the two largest counties using DREs, and accounting for the 5% recognition rate, by only shifting 7.7% of the voters (and thus 1.15 recognitions per machine). These numbers fall well within the normal bounds and are further supported by the fact that the two target counties voted 62 and 59 percent for Obama/Biden in 2008 (New York Times 2008). Therefore, the plan in North Carolina is to attack the EMSs of Mecklenburg and Guilford Counties for a 7.7% vote shifting presentation attack if the polls moved enough to warrant a potential loss by the Romney/Ryan ticket.

Therefore, the plan overall is: to attack via presentation attacks, 2 counties in Nevada at 5.5%, 3 in Ohio at 8.75%, 6 in Colorado at 11% and to put an attack against 2 in North Carolina at 7.7% on the back burner; to attack via the X% attack, 4 counties in Virginia at 9.5% and 8 in Pennsylvania at 11.2% (with an enforcement of 80-20 on provisional votes as well); and to get the attack code on the machines via outright attacking the EMSs in those key counties.

[36] Let f = 0.02*0.25 then Shift = (0.8f - 0.54f) + (0.48f - 0.2f) thus Shift = 0.0026.

Section 6.5: Firing on the Targets

"It isn't important who is ahead at one time or another in either an election or horse race. It's the horse that comes in first at the finish line that counts." – Harry S. Truman (Howington 2013).

With the plan in place, it is time to not only start writing the attack code and developing plans for gaining physical access to the EMSs, but also to watch the polls in order to ensure that they do not shift enough to cause a change in plans. Furthermore, since the attack vector is via physically accessing the 25 EMSs, which can be done as easily in the weeks leading up to the election as months before the election, it is wiser to wait to deploy the attacks until closer to the election so that the attacks can be based on the most accurate polls. In the end, the polls do not shift a large amount between early June and the weeks leading up to the election and the attack plan remains relatively intact as originally conceived, but a few key shifts greatly impact the result of the attack.

The first thing to explore, outside of perfecting the attack code, is to hire an accomplice to perform the break-ins given my lack of experience in the area. In fact, given the that at least 23 buildings need to be accessed in 5 states around the county (or 25 in 6 if North Carolina turns against Romney/Ryan), it is unlikely that I could physically access all of the buildings in a timely manner on my own. Therefore, I need two accomplices: one to attack the western states of Nevada and Colorado and the other to attack the three or four eastern states of Ohio, Pennsylvania, Virginia and possibly North Carolina. In fact data from Google Maps shows that attacking the western states alone would require 22 hours of driving time. From further analysis, given the clustering of the locations, I expect it to take somewhere in the neighborhood of five days to execute the attack in the west (Google Maps 2013).[37] The eastern route takes a similar amount of time with 4 days and 25 hours of driving time to access the buildings in Ohio, Pennsylvania and Virginia and adding in North Carolina adds 1 more day and 6 more hours of driving time (Google Maps 2013).[38] Therefore, the routes would start in Nevada and North Carolina or Virginia so that more last second attacks can be planned and executed on the states polling the closest to dead even, namely Ohio and Colorado.

[37] The full link will not fit in the word bibliography manager due to length requirements as such it is included here: https://maps.google.com/maps?q=from:Washoe+County+Elections:+1001+E.+9th+Street,Reno,+Nevada+89512+to:Clark+County+Elections:+965+Trade+Drive,+Suite+A,+North+Las+Vegas+to:Mesa+County+Elections:++544+Rood+Ave,+Grand+Junction,+CO+81501+to:Lake+County+Clerk+%26+Recorder,+Lake+County+Clerk+%26+Recorder,+505+Harrison+Ave,+Leadville,+CO+80461+to:Arapahoe+County+Elections+Division,+5334+South+Prince+Street,+Littleton,+CO+80120+to:Denver+County+Elections:+200+West+14th+Avenue+Suite+100+Denver,+Colorado+80204+to:Weld+County+Elections+Department,+N+17th+Ave,+Greeley,+CO+80631+to:Larimer+County+Elections,+West+Oak+Street,+Fort+Collins,+CO&hl=en&sll=38.401352,-112.247981&sspn=9.346237,21.643066&t=w&z=6

[38] The full link will not fit in the word bibliography manager due to length requirements as such it is included here: https://maps.google.com/maps?q=from:Mecklenburg+Board+of+Elections,+Kenilworth+Avenue,+Charlotte,+NC+to:Guilford+County+Elections+Brd,+Guilford+County+Elections+Brd,+301+W+Market+St,+Greensboro,+NC+27401+to:Virginia+Beach+Elections+Department,+Princess+Anne+Road,+Virginia+Beach,+VA+to:County+of+Henrico:+4301+E+Parham+Rd,+Richmond,+Virginia+23228-2745+to:Prince+William+County+office+of+voter+registration+and+elections,+9250+Lee+Avenue,+Suite+1%3B+Manassas,+Virginia+20110+to:Fairfax+County+Elections+Office,+Government+Center+Parkway,+Fairfax,+VA+to:York+County+Controller,+York+County+Controller,+28+E+Market+St,+York,+PA+17401+to:Montgomery+County:+Communications,+Montgomery+County:+Communications,+425+Swede+St,+Norristown,+PA+19404+to:Lehigh+County+Voter+Registration,+South+7th+Street,+Allentown,+PA+to:Northampton+County+Election+Office+670+Wolf+Ave+Easton+PA++18042-4343+to:Luzerne+County+Courthouse,+Wilkes-Barre,+PA+to:Westmoreland+Election+Bureau,+Westmoreland+Election+Bureau,+2+N+Main+St+%23+109,+Greensburg,+PA+15601+to:Allegheny+County,+Allegheny+County,+1520+Penn+Ave,+Pittsburgh,+PA+15222+to:Erie+County+CourtHouse,+Erie+County+CourtHouse,+140+W+6th+St,+Erie,+PA+16501+to:Franklin+County+Board+of+Elections+280+East+Broad+Street,+Room+100+Columbus,+OH+43215+to:Montgomery+Count+Elections,+451+W.+Third+Street++Dayton,+Ohio+45422+to:Lucas+County+Board-Elections,+1+Government+Ctr+%23+300,+Toledo,+OH&hl=en&sll=38.432684,-79.708464&sspn=9.341803,21.643066&t=w&z=6

With all of that planned, the next question is do the polls shift drastically? Figure 25 shows a five poll moving average of the poll numbers from May 19th to September 16th and from September 16th until November 5th, the day before the election. The June to Mid-September polls do not show a large amount of eventual variation amongst most states as while the polls jumped around a significant amount, they settle in around their original projected values. The one state that changes is Ohio, which while sometimes in Romney/Ryan's favor, seemes to regress to the mean of polling 4 points down, significantly more than expected. This takes Ohio out of contention even after the attack as in order to shift only 3% of the overall vote, I need to target 14 districts with an 11.2% vote changing attack. As such moving into Mid-September, my plan remains the same in all states but Ohio which needs to be investigated further.

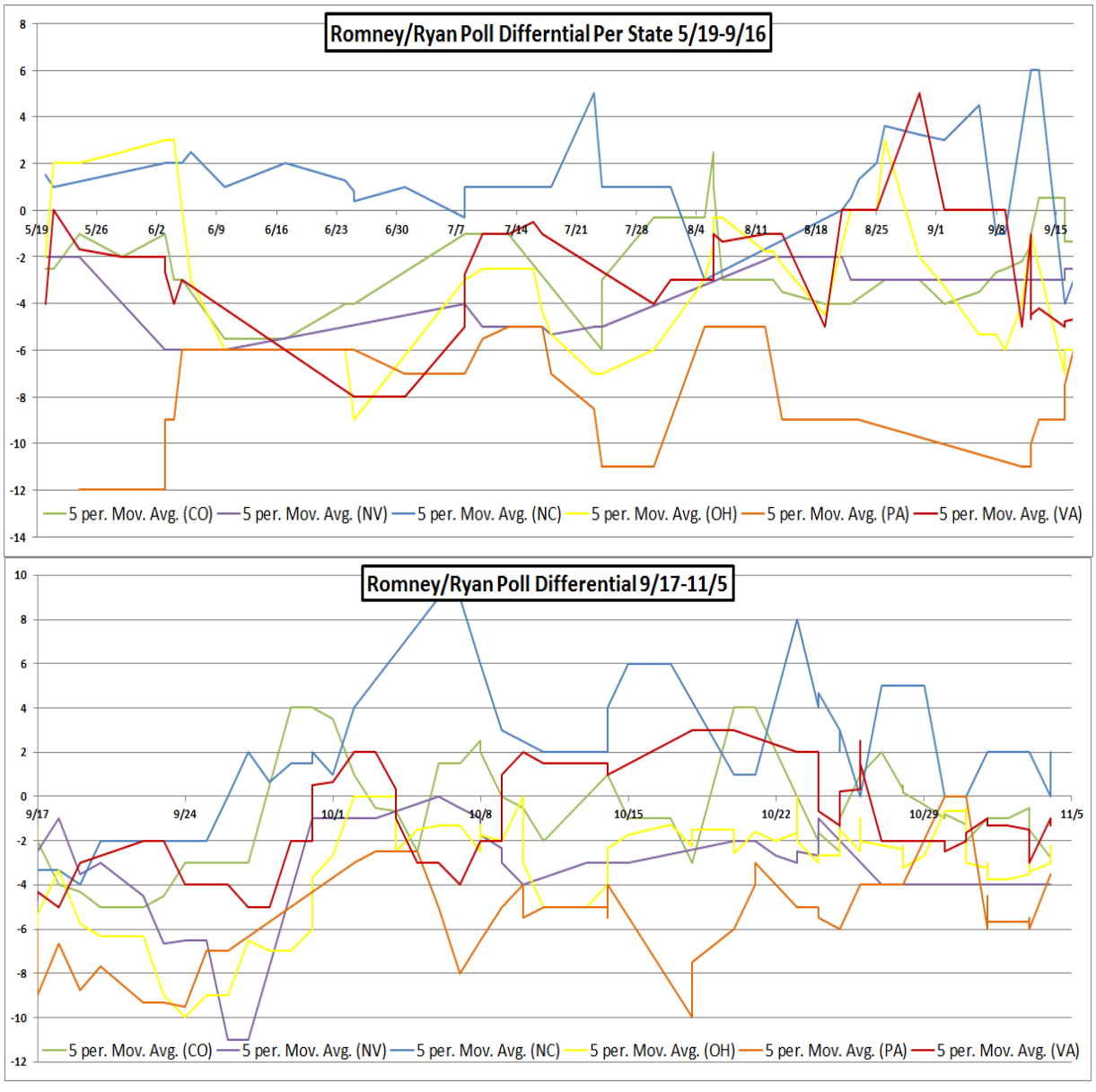

Figure 25: May to November Full Poll Data
(Elliott 2012)

It is right at this crucial juncture, on September 19th, with most states on a downward motion in their polling and Ohio proving to be problematic when disaster struck the Romney/Ryan campaign with the release of the infamous 47% video (Mother Jones News Team 2012). Fortunately, by the end of the first presidential debate on October 3rd, a decisive victory for Romney, the polls returned and in some cases exceeded the levels seen in early September (J. Rubin 2012). With one month to go before the election, and therefore less than three weeks to go before the release of the attacks, the values of the polls, contrasted from the May-June values, are shown below in Figure 26.

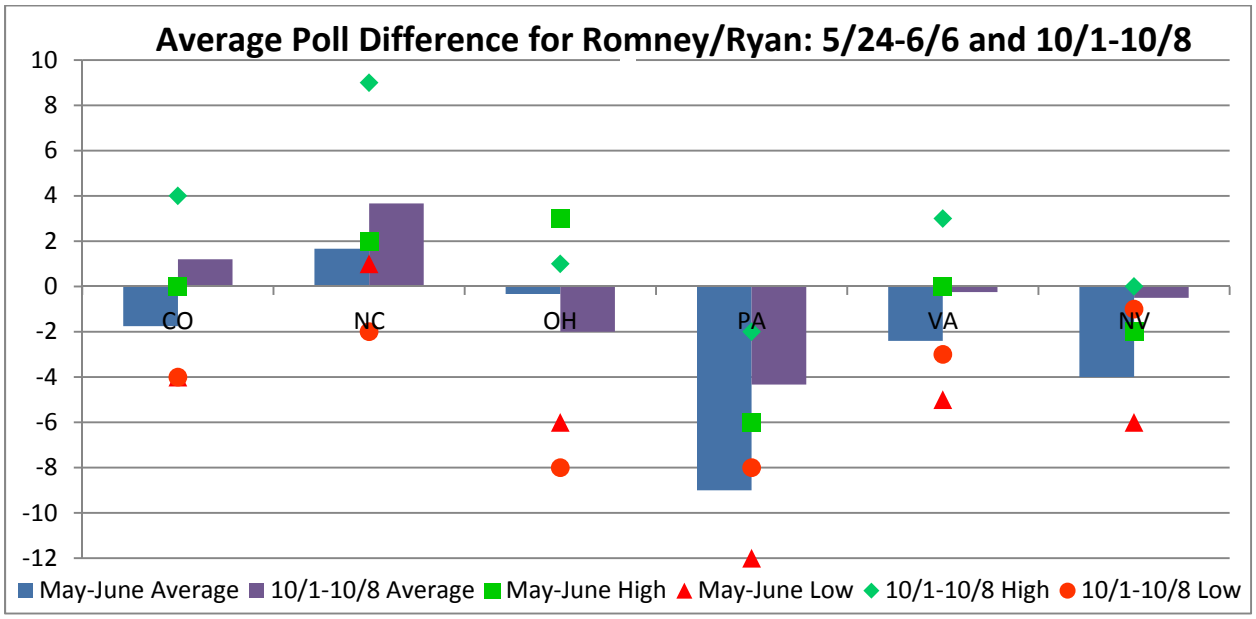

Figure 26: May-June vs. First Week in October Polls
(Elliott 2012)

This data is quite pleasing overall. North Carolina is even more in Romney/Ryan's favor further indicating no need to attack the state. Furthermore, Colorado, Nevada and Virginia all are polling almost dead even. This means that the planned attack on Colorado can now be predicted to succeed and the attacks on Nevada and Virginia can be paired down from attacking 4% and 2.4% of voters to more around 1%, making the attack much safer.[39] Also while the attack in Pennsylvania remains the same, the state is now only polling around 4 points down meaning that the attack will now potentially succeed. The only problem is that Ohio is still polling 2 points down. As such the planned 1% attack would have to be increased to 2% meaning that the number of counties needed to be attacked would double from 3 to 6 and the attack percentage would increase to 11%. It is then time to sit back again and watch the polls right up until 10 days before the election when I will make the final updates to my code and instruct my accomplices to start to deliver the attacks so that even if unexpected delays occurred, the attack could be carried out in time. In Figure 27 one can see the polls from 10 days before the election contrasted with the early October polls.

[39] In the case of Nevada this would mean dropping down the number of counties attacked from 2 to 1 and then attacking only 1.75% of the vote. In the case of Virginia, it would mean dropping the number of counties down from 4 to 1 as well and decreasing the attack to 8.25%.

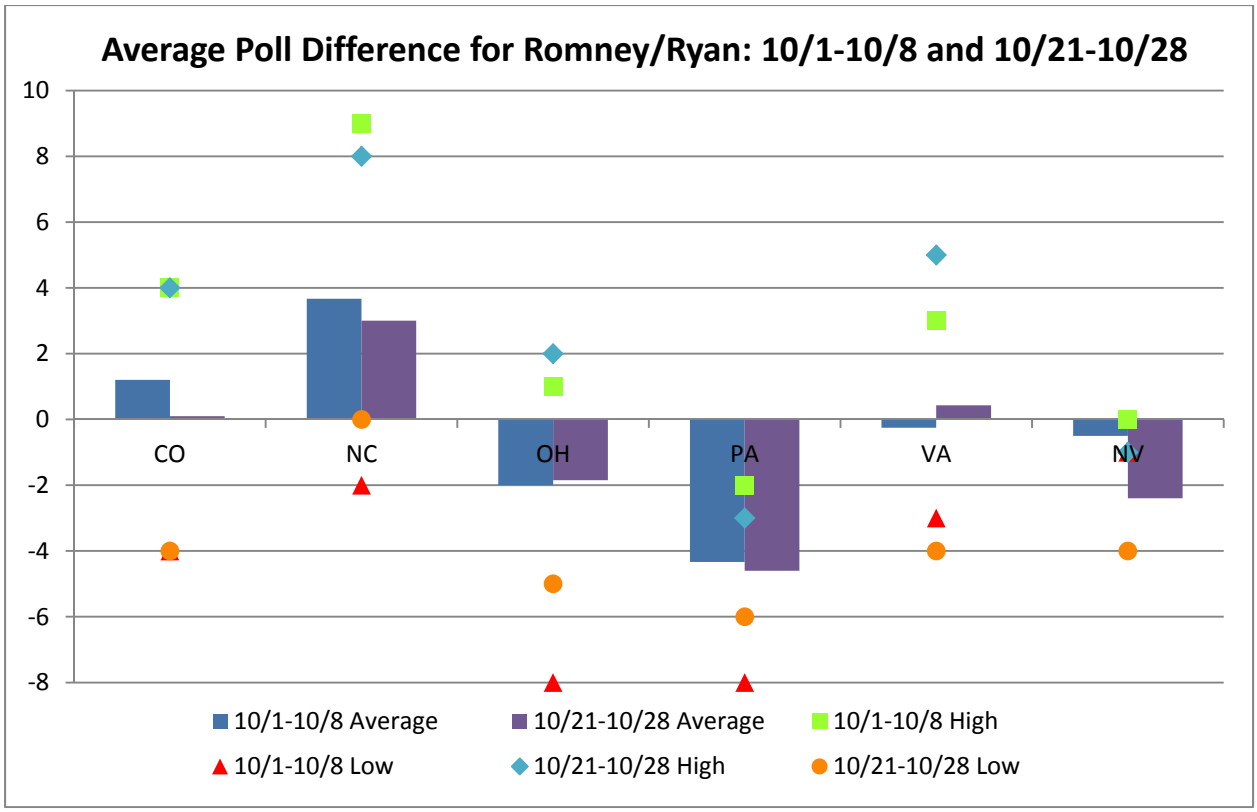

Figure 27: Change in October Polls
(Elliott 2012)

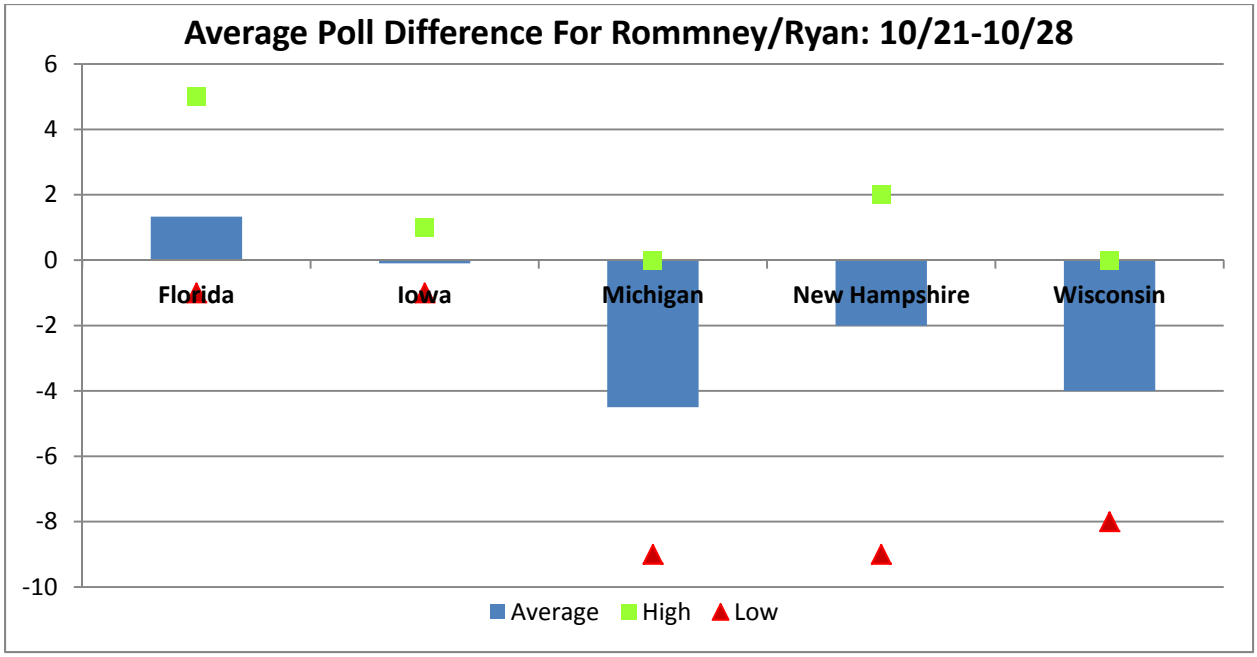

Figure 28: Non-Key Swing State Polls 10/21-10/28
(Elliott 2012)

From this last snapshot before I release the attacks, I can conclude that North Carolina can be ignored. Also, while it is unclear if the attack in Pennsylvania is going to be effective, it may succeed, thus the 3.75% attack will go as planned. While, Colorado and Nevada are back to polling at levels requiring that the original plans be executed to provide a comfortable margin of victory, the plan in Virginia can be scaled back from a 9.5% to an 8% attack. Releasing this final plan minus Ohio to my accomplices, I will continue to monitor Ohio with the objective of finalizing the final code and sending it to my accomplice 5 days before the election, once he finishes his attacks on the other eastern states.

However, before the accomplices are given the go ahead order, I will quickly check the polls in the other swing states in order to see if I can get away with attacking fewer states. From this data, shown in Figure 28, the only potential state that might be able to count on to fall for Romney/Ryan is Florida and its 29 electoral votes, which would allow me to ignore attacking Pennsylvania, and instead focus my accomplices' efforts on attacking more EMSs in Ohio. Therefore, I need to pull up some more data on the Florida polls, as a one point average margin is not enough to warrant calling off the low probability of success attack on Pennsylvania. Plotting out the entire poll data on Florida from September to October 28th, the actual pattern in the state becomes clearer and it actually appears that the poll numbers are regressing back to a dead even race as shown in Figure 29 below. As such, I sadly cannot count on a Florida victory and have to go ahead with the attacks as planned keeping a close eye on the Ohio polls and analyzing them with some statistical modeling packages to try to better predict how the state will vote on election day. An example of this type of analysis is shown in Figure 30.

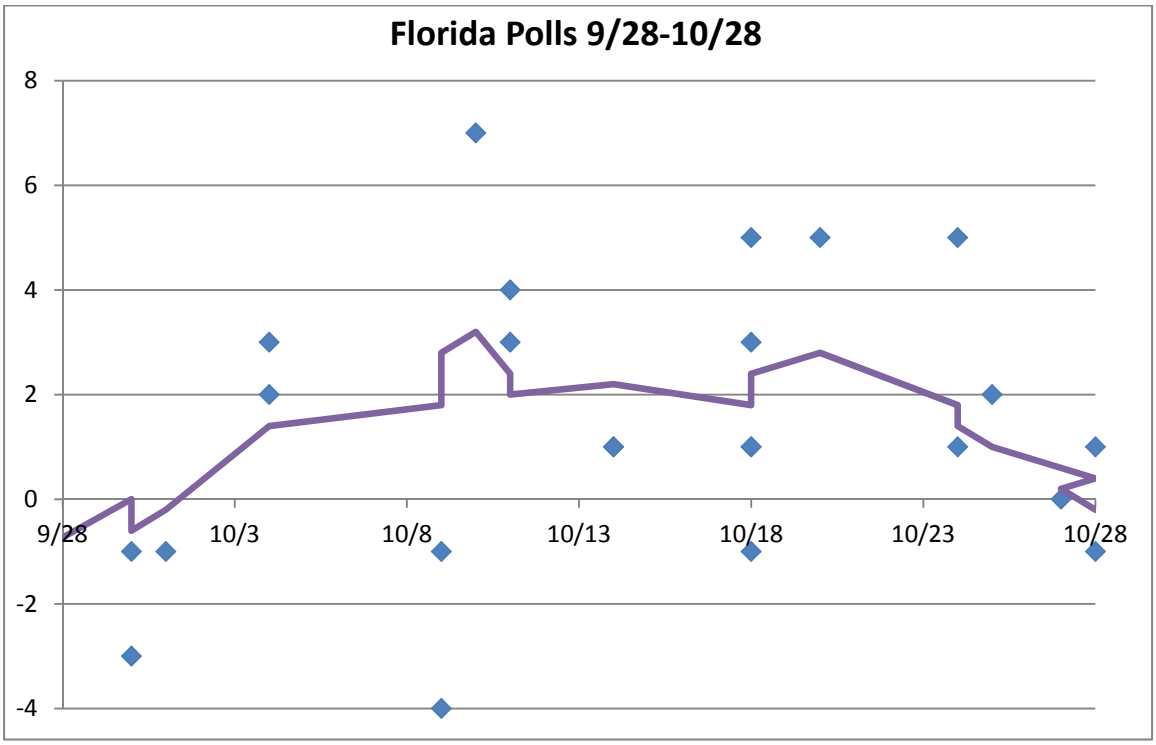

Figure 29: Florida Polls 9/28-10/28
(Elliott 2012)

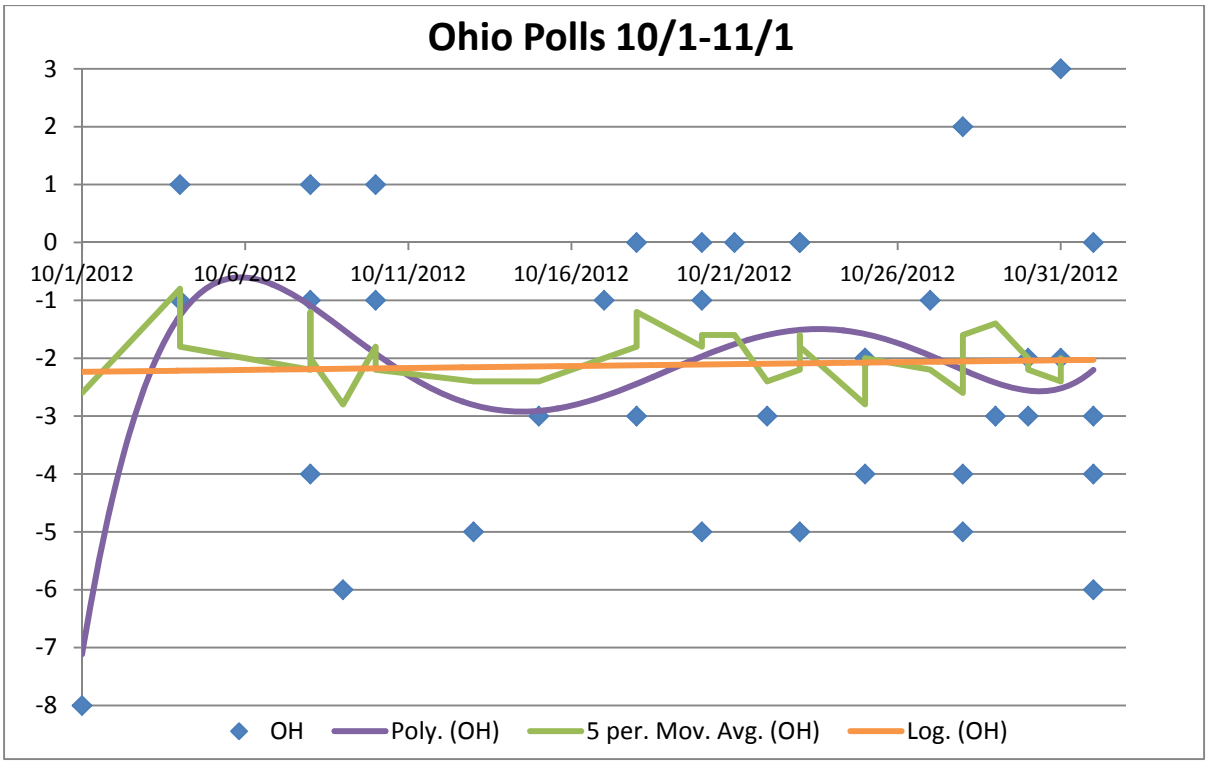

Figure 30: Ohio Polls 10/1-11/1
(Elliott 2012)

As Figure 30 shows, regardless of the type of basic modeling preformed, all of the various best fit lines hover in around two points down for Romney/Ryan. Therefore, I need to move around 2.5% of the vote in order to ensure victory. In order to pull this off I need to target 9 different counties with an 11.2% vote changing attack registering an average of 1.68 detections per machine. While these numbers are still within or near the bounds I set earlier they are not nearly as comfortably low as they were in the case of the 1% attack. This news while disheartening will not rule out the possibility of a victory, but will just raise the stakes in terms of detection as now 5 additional EMSs need to be physically accessed.

In the end there will be a total of 2 EMSs attacked in Nevada, 6 in Colorado, 4 in Virginia, 8 in Pennsylvania and 9 in Ohio for a total of 29 EMSs. Therefore, there are 29 chances in which the accomplices can be discovered. Given that crime statistics show that only 13% of burglars are caught and my accomplices are highly trained with a proven track record and are not stealing anything but simply obtaining access and inserting a USB memory stick into a computer, I believe it is safe to assume that the detection rate for the attack would be far lower than 13% (SecurityBase.com 2011). In fact, given that nothing was stolen, I think the detection rate could realistically be as low as 1%. Even still, with a 1% detection rate in all 29 accesses, the overall probability of accessing all 29 EMSs without being detected is only 75%.[40] As such, there is a relatively high chance that my final attack will be detected, but with no way around breaking into that many buildings all I can do is hope for the best.

[40] P(success) = (1-P(detection))^(number of attacks) = 0.99^29 = 0.747

The question is then, if my accomplices get away with inserting the attack code, will this attack actually swing the election. The 2012 election results show that Obama/Biden sweeps the swing states not considered for attack and Romney/Ryan takes North Carolina as expected, meaning that the only way the Romney/Ryan ticket can win the election is if all of the attacks are successful. To determine this I need to turn to the final election results and break it down by state and by county. Unfortunately, the reports from many states on how many voters chose to vote by mail or vote provisionally, etc. have not been released. However, even making the overly rosy assumption that 100% of voters in the attacked counties vote at the precincts, the results show that Obama/Biden dominates Election Day and as such the majority of the swing states are not even close. Therefore, even with these foolishly rosy assumptions, Colorado, Nevada, Pennsylvania and Virginia will be lost and as such the election will be lost as shown in Figure 31 below. The President and Vice President will be re-elected.

State	Votes Shifted	New Obama/Biden Total	New Romney/Ryan Total	Margin
CO	79,139	1,283,428	1,224,620	-2.3%
NV	46,932	507,907	487,033	-2.1%
OH	186,067	2,734,588	2,754,440	0.4%
PA	207,871	2,886,339	2,784,369	-1.8%
VA	19,295	1,962,172	1,832,170	-3.4%

Figure 31: Final Attack Results
(CNN 2012)

Chapter 7: The Aftermath and Lessons Learned

"All technology, no matter how advanced, is going to be vulnerable to attack to some degree. The history of attacks on voting systems teaches us how foolish it would be to assume that there will not be attacks on voting systems in the future. But we can educate ourselves about the vulnerabilities and take the proper precautions to ensure that the easiest attacks, with the potential to affect the most voters, are made as difficult as possible. Good threat analysis allows us to identify and implement the best security precautions." - Brenan Center for Justice (L. Norden, The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost 2006, 20)

As revealed in Chapter 6, stealing a presidential election in the United States is not an easy task. Since attacks cannot steal very large portions of the vote, the attacking candidate needs to do well in the election in order to be in a position to be aided by the attack. As such, the country is fairly safe from an attack against a presidential election. However, with many congressional races occurring in only a handful of voting districts, these smaller scale elections may be easily attacked as gaining access to one key EMS and switching a very small percentage of the vote may be enough to swing the election. Furthermore, small scale elections have been shown to be vulnerable to many other varieties of attacks that had to be ruled out for my attack on the presidential election due to scalability concerns. Therefore, it is important to consider how the flaws in the various voting systems can be fixed in both the short and long term in order to ensure better, safer elections.

Section 7.1: The Short Term

"The economic downfall of the past decade has left precious few resources available for further improvements to the nation's voting processes." – Dean C. Logan, Registrar-Recorder/County Clerk, Los Angeles County (Alvarez, Ansolabehere, et al. 2012, 64)

As evidenced by the above quote, PCOS, DREs with and without VVPT, and vote-by-mail systems will be the main forms of voting for the foreseeable future and districts with PCOS machines are unlikely to switch over to DREs and vice versa. This therefore begs the question: how can these systems be better secured today? From exploring the various attacks against the systems, and attempting to deploy them in the previous chapters, it is apparent that effective audits are a great stop-gap measure to prevent and discourage attacks, and as such paper trails are very important. Furthermore, it appears that testing the machines for accuracy before and after elections, while potentially helpful to catch bugs in the software, is fairly useless in discovering attacks and new testing methods must be employed. Finally, proper protections need to be put in place to prevent the scaling of attacks. Therefore, with audits, better forms of testing and impediments to scaling in place, elections can be secured in the short term.

With regard to paper trails and audits, the news is promising as audit and paper trail laws are on the rise, and of the eleven swing states analyzed in this thesis, all but two of them have paper trails in use in their states. That said the nation is not where it needs to be today. According to the report "Counting Votes 2012: A State by State Look at Voting Technology Preparedness," the states of Arkansas, Colorado, Delaware, Georgia, Indiana, Kansas, Kentucky, Louisiana, Maryland, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee, Texas, Virginia all receive a rating of inadequate with respect to the usage of paper trails. While this seems like a disastrously large amount of states, the report overstates the danger. For example, Colorado makes the list due to the fact that Jefferson County uses DREs without VVPT for its accessible voting machines which will be primarily used be the visually impaired who could not check the VVPT anyway (Goodman, Mulder and Smith 2012). Despite this

exaggeration, federal law needs to be put in place to require that all the states use standard polling place equipment that provides and auditable paper trail. Fortunately, H.R. 12 (and its companion bill S. 123), the Voter Empowerment Act of 2013, addresses this issue as Section 601 mandates the use of a voter verified paper trail as follows:

1. The voting system shall require the use of an individual, durable, voter-verified, paper ballot of the voter's vote that shall be marked and made available for inspection and verification by the voter before the voter's vote is cast and counted, and which shall be counted by hand or read by an optical character recognition device or other counting device. For purposes of this subclause, the term `individual, durable, voter-verified, paper ballot' means a paper ballot marked by the voter by hand or a paper ballot marked through the use of a nontabulating ballot marking device or system, so long as the voter shall have the option to mark his or her ballot by hand.
2. The voting system shall provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved in accordance with [the above] clause.
3. The voting system shall not preserve the voter-verified paper ballots in any manner that makes it possible, at any time after the ballot has been cast, to associate a voter with the record of the voter's vote without the voter's consent. (H.R. 12 2013)

This ensures that a paper trail will be in place in all voting machines throughout the country and importantly will also authorize federal funding to pay for the necessary upgrades to the voting system.

However as exemplified in this work, and as best explained by the Brennan Center for Justice, "Systems with voter-verified paper records provide little, if any, security benefit over systems with such records, unless there are regular audits and/or recounts of the paper records (L. Norden, The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost 2006, 26)." Audits need to be performed and they need to be performed well. According to the report "Counting Votes 2012: A State by State Look at Voting Technology Preparedness," one half of the states use of audits is inadequate and another 13 need serious improvement (Goodman, Mulder and Smith 2012). This is quite disturbing but not surprising as audits are expensive and time consuming. However, as shown in the Brennan Center's Report, "Post Election Audits: Restoring Trust in Elections," well designed statistical audits can actually be performed in a cost effective and secure manner through hand counts of the paper trails (Norden, Burstein, et al. 2007), and therefore audits should be required at a national level. Fortunately, not only does the Voter Empowerment Act of 2013 mandate in section 611 that audits automatically occur in close elections, but it also uses the best statistical practices for determining how many ballots must be audited. The bill also goes on to specify best practices for performing an audit and importantly, authorizes the use of federal funds to pay for the state's expenditure on the audit (H.R. 12 2013). If passed into law the Voter Empowerment Act of 2013 will greatly secure elections through mandatory paper trails and audits.

If these measures are adopted, the only vote changing attack remaining will be the presentation attack making voter education paramount. If the dismal notification rate of attack climbs from 3% to only 20% of voters, only 3.33% of votes on a given machine could be switched in order to stay below the projected 2 recognitions of the attack per machine. Since in the attack scenario in the previous chapter at least 5% of voters were needed to be attacked per machine to swing a state, this would prevent most attacks from succeeding. Therefore, having these paper trail and audits in place and educating voters can have a large impact on election integrity in the short term.

With regard to better testing methods, the answer is parallel testing. With parallel testing a few machines are randomly pulled out of randomly chosen precincts on Election Day and brought to an alternate facility where under the careful eye of a handful of election officials, these machines are voted on by the officials throughout the day to simulate normal election procedures. Therefore, any deviations in the behavior of the machine and its final tallies will be carefully observed and monitored and unlike when the machine is put into testing mode, there are no clear programmatic cues to warn the attack code that this is occurring. While Professor Rubin states, "The point of parallel testing is to fool any malicious code that was written to perform properly in a test but to cheat in an actual election…The challenge is to mimic those conditions exactly so that the software will not recognize it is engaged in a test rather than the real thing (A. D. Rubin 2006, 180-181)," and goes on to show how there are actually many ways in practice that a machine may be able to tell that parallel testing is occurring,[41] proper testing guidelines can be written to ensure effective parallel testing. Such testing would then observe attacks in real time and allow election officials to potentially notice the attack early enough to make a copy of the code on the machine before the attack code had a chance to delete itself. While parallel testing is not in place in most states, and is not contained in the Voter Empowerment Act of 2013, I firmly believe that parallel testing should be mandated by federal law. As the Brennan Center for Justice aptly states: "Parallel Testing creates a kind of arms race between attackers and defenders: as Parallel Testing becomes more sophisticated, the attacker must become more sophisticated (Norden, Lazarus, et al. 2006, 60)." Therefore, parallel testing can raise the stakes for attackers and discourage them from attempting an attack.

With regard to scaling attacks the three vectors which have to be better protected are: the voting machine companies, the EMSs, and the wireless components on machines. With regard to the voting machine companies, the quick fix is to prevent the companies from pushing software updates starting a month before the election. Attackers will then be forced to either base their attack on potentially stale polls or chose another attack vector. As such, this requirement should be added to the Voter Empowerment Act of 2013. Despite the inevitable protest from companies that it would inhibit their ability to fix a critical flaw found close to Election Day, it might also force these companies to be more prudent with the testing of their code to ensure that the critical bugs were found ahead of time which might have the side effect of the improve the quality of code on the machines.

With regard to attacks against the EMSs, the main topics that need to be considered are the security of election headquarters and the access of insiders. With regard to election headquarters security, the EMS must never be attached to the internet or intranet and should not possess a wireless card because as Alvarez and Hall state, "As long as the computers associated with voting or tabulation are, or at some point have been, connected to any network, they suffer from [grave] risk (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 92)." The EMS should also have its hard drive completely wiped in between elections and a fresh version of both the operating system and the election management software should be installed to ensure that it is free of viruses and running a trusted version of the election management software, and all removable media should also go through a similar

[41] For example, in many current testing scenarios one token is repeatedly used to validate a voter instead of the many tokens used in a real polling location (Norden, Lazarus, et al. 2006, 54).

sanitation process. The EMS must also be stored in a secure location throughout the election process to prevent an attacker from being able to gain physical access to the device. If the EMS is sufficiently secured in these ways then the only way for an attacker to compromise the EMS would to be through compromising an insider.

With regard to the power of insiders, careful attention has to be made to system design to ensure that they are given as little power over the election results as possible and that when they are in complete control, there is someone else present keeping them honest. This is because with the help of election officials an attacker can easily infect the EMS without breaking into any buildings and can have the code deployed the night before the election. Furthermore, throughout the day poll workers can be instructed to "run a diagnostic program" on the machines and update the attack in real time and after the attack, paper trails can be destroyed. Therefore, no election official should be allowed to access the EMS alone. Most districts have both a Republican and Democrat head election official in order to keep the ballot design and absentee ballot counting process honest. These officials should also each hold separate keys to access the EMS. Furthermore, there should be constant pairing of election workers whenever election materials are being transferred. Finally, voting machine software should ensure that only with the supervision of multiple poll workers can a machine's settings be updated during an election. Therefore, while insiders will always have privileged access to sensitive materials, ensuring a "buddy system" between members of each leading party will lead to self-policing and prevent many attacks.

With these protections in place the only way to scale an attack would be through wireless access. As such, all machines that have wireless cards in them should have these cards removed. They serve no beneficial purpose and simply pose a security risk today. If these simple steps are taken the bar will be raised so high that an attack is unlikely to be successful unless a race is so close that it comes down to only a couple hundred votes in one state. If that was the case, then there are many lower tech attacks, such as simple vote buying, which can be equally as dangerous. Therefore, through these recommendations elections can be greatly secured in the short term. It is imperative that the Voter Empowerment Act of 2013 is amended to include all of these provisions, has the timeline of enforcement of these rules moved up to the 2014 elections, and is passed. Unfortunately, given the size of the bill, controversy over certain sections could slow it down and since the Supreme Court just took a stand against federal control over election laws (albeit in a case where only certain states were targeted) this passage is not guaranteed (Liptak, Voting Rights Law Draws Skepticism From Justices 2013). Therefore, pressure must be put on congress to ensure at least the passage and installation of the previously mentioned security related sections of the bill.

Section 7.2: The Long Term

"It's always going to be hard to stop James Bond. But I want to move it to the point where grandma can't hack elections, and we're really not there." –Roger Johnston, head of the Vulnerability Assessment Team at Argonne National Laboratory (Johnston 2012)

In the long term it is clear that the nation is in need of new systems that can improve the usability and transparency of the current voting systems and at a lower cost while ensuring privacy. For starters, at the system design level, national ballot design laws should be put in place to ensure that all ballots meet top standards for ease of use and accuracy of voting. Furthermore, voter interaction with voting machines should be standardized so voters can become accustomed to standard error messages and voting machine behavior in order to further prevent voter error. Also, poll workers need to be better trained so that voting operations run smoother. Beyond that, process must be put in place to allow voters easier access to the polls and new classes of voting machines need to be developed to ensure an improved and more secure voting system.

Figure 32: A Cartoon on Technology and Voting Today
(Luckovich 2012)

The expansion of early voting in section 801 of the Voter Empowerment Act of 2013 will help alleviate the issue of voters being unable to access the polls as voters will have many days, including the preceding weekend, to vote. This is shown below:

1. In General- Each State shall allow individuals to vote in an election for Federal office not less than 15 days prior to the day scheduled for such election in the same manner as voting is allowed on such day.
2. Minimum Early Voting Requirements- Each polling place which allows voting prior to the day of a Federal election pursuant to subsection (a) shall--
    a) allow such voting for no less than 4 hours on each day (other than Sunday); and
    b) have uniform hours each day for which such voting occurs.
3. Location of Polling Places Near Public Transportation- To the greatest extent practicable, a State shall ensure that each polling place which allows voting prior to the day of a Federal election pursuant to subsection (a) is located within walking distance of a stop on a public transportation route. (H.R. 12 2013)

However, early voting at 4 hour days is not a panacea and as such other considerations should continue to be analyzed. Along those lines voter registration and absentee ballot requesting needs to be modernized to make it easy for all Americans to become eligible to vote. These topics could become dissertations themselves and thus I will not dive further into them at this time. However I will explore what the future of precinct based voting and vote-by-mail systems may become to ensure that future systems are usable, transparent, private and cost effective.

With regard to the future of precinct based voting systems, it is important to ensure that future voting system designers keep all four forces in mind and fortunately districts are turning to security researchers to help ensure that this occurs. In fact, Rice University Professor Dan Wallach is working with Travis County, Texas to design a next generation voting system. His team's design resulted in the primary voting machine being a touchscreen and audio enabled BMD which stores an encrypted version of the vote total via cryptographic chaining[42] and then prints out a two part ballot. The voter is then given a choice to either audit the ballot or vote the ballot. If the user votes the ballot the plaintext half of the ballot is scanned by a PCOS machine and the encrypted half is taken home and used by the voter to check that the vote actually made it into the final count as all the encrypted halves of the cast ballots are posted on a website. If the user instead decides to audit the ballot, then the voter will bring both halves home and can later decrypt the encrypted half to ensure that the machine was encrypting votes correctly (Stark, et al. 2012). This system is therefore auditable in a variety of ways through not only the electronic and cryptographic total comparisons and through the audit of the paper ballots, but also through individual voters' audits. It is also quite usable as it is based off of a very user friendly and handicapped accessible BMD. That said, it is possible that many voters will get confused by the many options and steps and the increased machinery in precincts may make it quite expensive. Therefore, while this may not be the exact precinct based voting system of the future, it shows that future voting systems can be designed to balance the four key forces of usability, transparency, privacy and cost.

Before I finish discussing the future of precinct based voting systems there are a few specific features and design patterns that need to be discussed. For one, no machines should have wireless cards or capabilities. Secondly, better back up batteries with hours of usage time should be included on machines to prevent denial of service attacks and given the battery life of most laptops, tablets and phones today, this does not seem like a lot to ask. These next generation systems should also be developed in an open source manner. While many companies insist on security by obscurity, history has shown that the source code has become public knowledge regardless of their efforts to keep it secret. Open source development would allow for security researchers to actively look at the code and catch many flaws improving the systems security. This move is also not unprecedented as the entire country of Australia votes on the same voting machine which was developed via an open source project in 2003 (Zetter, Aussies Do It Right: E-Voting 2003). As a final note, regardless of how well designed the next generation precinct based voting systems are, one must keep in mind that the poor economics of the voting machine market ensure that these systems will not be designed by the top software engineers as the voting machine companies do not have the funds to higher the top talent. However, if states decide

[42] This ensures that even a corrupted system can only change its future and not its past as each vote is continuously appended to the encrypted history of all previous votes and then encrypted (Stark, et al. 2012).

to purchase machines and service packages on a state-wide scale,[43] the market could begin to stabilize and the companies could begin to improve their talent. Fortunately, the Voter Modernization Act of 2013 also includes provisions to provide funding for the research and development of new voting machines further helping in this endeavor. That said more research needs to be done on ways to improve the voting system market.

At the same time that precinct based voting is being analyzed and improved upon it appears that no fault absentee balloting is on the rise. This will lead to many states being in a partial vote-by-mail situation. This sentiment is observable in Section 801 of the Voter Empowerment Act of 2013:

"In General- If an individual in a State is eligible to cast a vote in an election for Federal office, the State may not impose any additional conditions or requirements on the eligibility of the individual to cast the vote in such election by mail, except as required under subsection (b) and except to the extent that the State imposes a deadline for requesting the ballot and related voting materials from the appropriate State or local election official and for returning the ballot to the appropriate State or local election official (H.R. 12 2013)."

Therefore, the future of remote voting (voting from outside of a precinct) must be carefully analyzed. While vote-by-mail systems reduce the cost of an election and remove polling place accessibility issues, they also may reduce or even eliminate voter privacy. Will this trend to vote-by-mail systems be the step that swings Professor David Wagner's pendulum of privacy too far and lead to massive amounts of fraud, or will this simply reduce costs and allow more access to voting? While predicting an answer to that question is quite difficult, it does raise the concern that the nation is potentially become too comfortable with remote voting and is forgetting its past filled with bribery and intimidation. Election officials must keep these privacy concerns in mind moving forward and also need to find a way to ensure that remote voting can be done from a more user friendly interface than the current paper ballots. Finally, election administrators need to keep in mind that authenticating users who are voting absentee is very difficult and signatures can easily be forged. In fact, news recently broke that in the 2012 primary election in Miami-Dade County, Florida there was an attempt to register over 2,000 fraudulent absentee ballots (Mazzei 2013, Fineout 2013). While this suspicious behavior was detected and the ballots were ultimately not sent out, this does raise the possibility of a more sophisticated attack in the future. Therefore, these issues must be kept in mind as vote-by-mail is expanded across the United States through no fault absentee balloting.

[43] While this would centralize the risks into few voting machines, as shown in the previous chapter, the big companies already dominate the market and already provide scaling opportunities in many states.

Section 7.3: Internet Voting

"We did not believe SERVE [the DOD internet voting experiment] could be fixed through simple design changes; nor could we propose a viable alternative Internet-based system (Rubin 2006, 171)."

"The real barrier to success is not lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, and the goal of a secure all-electronic remote system, the [SERVE Project] has taken on an essentially impossible task. There is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough (Alvarez and Hall, Electronic Elections 2008, 84)."

A discussion of the future of voting, and especially of remote voting, would be remiss without a discussion of internet voting, and since an entire dissertation can be written on the subject, I will try to condense the topic down to the most salient points. The online voting movement is fueled by new laws such as the 2010 MOVE Act requiring states to give overseas military voters an option for electronic submission (Whitmer 2012), and half of the states already have some form of electronic return system in place (Hansen 2012, 163). At the same time, famous computer scientists such as Ron Riverest from the MIT/Cal Tech Voting Project consider internet voting to be comparable to connecting your toaster to a high tension power line (Rivest 2012). I believe at this time while internet voting does represent the future, and allows for voting systems to provide the usability of DREs to remote voters at a potentially even more reduced cost than vote-by-mail, there is no secure way to implement a fully functional system today. That said I would encourage research and development into partial systems to be deployed today and for complete systems to be deployed in the future when the world's understanding of cyber security has improved because as Alvarez and Hall aptly state, "The question is not whether the Internet should be used for elections, but when (Alvarez and Hall, Point, Click, and Vote: The Future of Internet Voting 2004, 27)."

Internet voting possesses many positive qualities, as it is the height of convenience and usability at a very low cost to states. Internet voting, like DREs, is software based and therefore not only boasts improved user interfaces but can also provide multilingual and audio support to voters, and can be further customized to reflect state specific voting regulations. By upgrading the current absentee paper balloting to the programmable user interfaces, thousands of voter errors can be reduced. Also, as over 94% of Americans report having internet access, this system has been theorized to effectively enfranchise hundreds of thousands of new voters around the country by reducing the challenges of reaching the polls on Election Day (Tedeschi Autum 2006). In fact, reports from the 2004 internet voting primary experiment in Michigan show that two thirds of voters chose to use the internet option solely for convenience purposes and over 90 percent of those who chose the internet option voted from their home computers (Alvarez and Hall, Electronic Elections 2008, 97). Internet voting also continues to have all of the cost reductions of vote-by-mail as all voting is done remotely and ballots do not even have to be mailed out to voters. Finally, internet voting allows military and overseas voters who do not have the ability to access the mail, and thus ability to vote absentee, to be able to vote. This is best exemplified by all the military personnel who find themselves on long undersea tours on submarines where there is absolutely no access to the outside world save through telecommunications. Clearly, there are some strong reasons why internet voting should be used in America today, unfortunately, there are equally damming security concerns.

Internet voting, due its remote nature, raises major privacy concerns. By effectively transforming homes and libraries into personal precincts, voter privacy can no longer be ensured by the state. More importantly, the integrity of the ballot is put into serious question. These integrity issues arise mainly from three properties of the internet itself: it has no paper trail, it is exceedingly scalable and it provides very little ability to authenticate users.

Lack of paper trails implies lack of auditability and therefore lack of ability to notice an attack. The response from the computer security community has been a whole host of cryptographic developments focused on verifying votes. These end-to-end (e2e) verification schemes are designed to ensure that once a vote leaves a voters machine it can be proven that its encrypted version had safely arrived at election headquarters. This is usually done by having the election tabulation software post to a public bulletin board all of the encrypted votes it receives. In this way, voters can check that their personal encrypted ballot made it to the billboard and thus to the tabulation software. Further developments in encryption algorithms have resulted in the development of mixnets in which all votes are pseudo-randomly shuffled and detached from voter identifying information before being decrypted for tabulation and homomorphic encryption schemes which allow votes to be tallied while encrypted and then only decrypt the final tallies ensuring voter privacy (Adida, Advances in Cryptographic Voting Systems 2006).[44]

While these advances make elections significantly safer and provide much better guarantees of integrity once the vote is encrypted and sent, none of the systems allow the user to decrypt their vote (for good reason to prevent anyone from decrypting any vote and then breaking voter privacy) and therefore the voter still must trust the algorithm to accurately encrypt the vote. In fact, Harvard/MIT's Ben Adida's online voting system Helios was found to be attackable from a malicious Firefox extension that abuses this exact fact. By manipulating the browser, researchers from University College London were able to change the vote right before it was encrypted. Therefore, the voter would see that their plaintext vote was correct and that the encrypted vote was correctly sent to the system, but would not know that the encrypted vote did not actually contain their plaintext vote (Adida, Helios: Web-based Open-Aduit Voting 2008, Adida, de Marneffe and Pereira, Helios Voting 2012, Estehghari and Desmedt 2010). Furthermore, even if these cryptographic protections were put in place, it is not clear that the average voter or election official would either trust or understand the complex math behind most encryption schemes and therefore be willing to adopt the technology (Alvarez, Ansolabehere, et al. 2012, 75). As such despite security researchers' best efforts internet voting lacks the robust protections provided by a physical paper trail.

Making matters worse, internet voting provides incredible scalability of attacks as the entire voting system is accessible from an attacker's home computer. Therefore, attacks would not need to be physically installed in each voting machine or loaded into each district's EMS but instead could be spread from the comfort of an attacker's couch. Furthermore, these attacks are easy to impliment as web applications are very brittle and automated processes can be used to isolate an error in one line of code in order to gain root access to the entire system (Alvarez and Hall, Point, Click, and Vote: The

[44] Homomorphic encryption unfortunately has a huge flaw as it removes the possibility of write in candidates which has been an important part of the American electoral process.

Future of Internet Voting 2004, 78-79). This is exactly what happened to the 2010 Washington D.C. internet voting experiment as single input was not escaped correctly which allowed a shell injection attack to compromise the election servers (Wolchok, et al. 2012). Making matters worse the internet also provides a wealth of opportunities for deadly distributed denial of service attacks (DDOS) which can be used to take down access to the voting website for certain key areas in the country and thereby depressing their vote totals. And while DDOS attacks are defendable, they have been successful at taking down major websites such as the Department of Justice and FBI (Perlroth 2012).

Finally, internet voting makes authentication of voters very difficult. The internet was designed to be a decentralized network resilient to attack making in-channel authentication very difficult. This poses a major threat to internet voting as it is very hard to ensure that the logged in voter is actually the one voting. Consequently, the Washington D.C. online voting experiment gave up on a pure online solution and ensured that only registered voters were voting by mailing a password to each voter thus reducing the system to an almost hybrid internet and mail system (Wolchok, et al. 2012). Furthermore, from the other side of the verification issue, there is no proof from a user that they have arrived at the correct voting website. In fact in reviewing the Department of Defense's attempt at an internet voting system, SERVE, Professor Rubin said the following with regards to such phishing attacks:

"Once voters had arrived at the phony site, even the most brilliant security system back on the real SERVE site would be meaningless. Whoever set up the fake site could just take the voter's passwords, log on to the real site, and vote however they chose. SERVE contained no countermeasures or protection against this sort of attack. [And importantly,] as far as I knew, none existed (Rubin 2006, 167)."

Therefore, in conclusion I believe that the United States is not ready for a full scale internet voting system today. However, hybrid solutions should be put in place so that researchers and election officials can begin to experiment with online voting so that it can be used in the future. Fortunately, the money allocated for voting system research by the Voter Empowerment Act can be used in this manner.

Before I leave this section, I would like to give an example of a hybrid system that can be deployed today as a platform to develop a full internet voting system. This system is called IPSnail, and is system I developed at the end of last year (Plancher and Pradhan 2012). The inspiration behind IPSnail is Professor Rubin's dream voting system, an electronic and paper hybrid system (Rubin 2006, 208), and the Washington D.C. experiment, which resorted to mailing voters a password to log onto the system. With IPSnail voters begin by registering to vote online. The list of registered voters would then be publicly available for review allowing for the eligibility verification of the voter rolls to be crowd sourced. Once voters are registered to vote with a valid home address, they are mailed a return envelope and a one-time-use password which is printed in both braille and normal type. Voters then use this code, in addition to their account credentials they set up during registration, to log into the system. This two factor authentication system is at least as secure as the current absentee and vote-by-mail voting systems which simply send an official ballot to the registered address.[45] Furthermore, moving to a two

[45] In recognition of the fact that many states are moving to stricter forms of voter ID, the system's log in criteria can be augmented by requiring that voters also give their driver's license number, or further verification methods as defined by the state. In the future, as bandwidth speed grows in rural areas, the system could also provide photo identification through video conferencing. However, this is impractical with current internet speeds.

factor authentication method is considered best practice by other nations using internet voting systems (Esteve, Goldsmith and Turner 2012, 57).

Once logged in, users are presented with the appropriate ballot and are guided through the voting process. Carefully designed warnings and error messages would prevent over-votes and warn against under-votes. Once the user has finished voting, the user will be instructed to print out his or her ballot and verify that his or her vote is recorded correctly. Then the user will be instructed to place the printed ballot in the return envelope and mail it back for tabulation. Through this key step of printing out and reviewing a paper record of the vote and then sending that to election headquarters for tabulation, an accurate paper trail is ensured. As such all programmatic attacks on the browser, online software, home computer, or printer can be detected and prevented. Furthermore, with a paper trail in place scaling attacks against this system would become very difficult.

While this system does not currently have a solution for the DDOS problem, the complaint that the hybrid solution still disenfranchises military members who are not reachable by mail is unfounded as the system would allow fully online voting via the SIPRNet (the SECRET level intelligence network). The security issue with internet voting comes from the inability to trust the user's device and the central server. Use of the SIPRNet solves these security issues as all devices on that network can be trusted, and if the SIPRNet is being compromised, there are larger national security issues than votes being switched. Therefore, through the use of hybrid systems like IPSnail, election officials and security reserachers can begin to experiment with safe versions of internet voting and determine how to better design internet voting systems for the elections of tomorrow.

Section 7.4: Concluding Thoughts:

In conclusion, there is no perfect voting system out on the market today, but there are some key steps that can be made as highlighted in Section 7.1 to provide stop gap measures to make the current voting systems secure today. There are also key insights and ideas that need to be kept in mind while developing the next generation of voting systems as highlighted in Sections 7.2 and 7.3 to ensure the security of future elections. One can safely conclude that if the Voter Empowerment Act of 2013 is amended to include all of the provisions mentioned in this chapter and is passed and if the research and development of future voting systems are done with all of the lessons learned from the past in mind, keeping a balance between usability, transparency, privacy, and cost, elections will be secure.

Bibliography

"2012 California Presidential Results." *Politico.* November 19, 2012. http://www.politico.com/2012-election/results/president/california/ (accessed December 5, 2012).

Abdelkader, R., and M. Youssef. "UVote: A Ubiquitous E-voting System." Vancouver, Canada: Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2012.

Abdullah, Halimah. "As Election Day nears, voter ID laws still worry some, encourage others." *CNN.* October 12, 2012. http://edition.cnn.com/2012/10/12/politics/voter-laws-update/index.html (accessed December 25, 2012).

Adida, Ben. *Advances in Cryptographic Voting Systems.* Cambridge, MA: Massachusetts Institute of Technology, 2006.

—. "Helios: Web-based Open-Aduit Voting." San Jose, CA: USENIX Security Symposium, 2008.

Adida, Ben, and C. Andrew Neff. "Ballot Casting Assurance." Berkeley, CA: Electronic Voting Technology Workshop on Electronic Voting Technology Workshop, 2006.

—. "Efficient Receipt-Free Ballot Casting Resistant to Covert Channels." Montreal: Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, 2009.

Adida, Ben, Oliver de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios." Montreal: Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, 2009.

Adida, Ben, Olivier de Marneffe, and Olivier Pereira. *Helios Voting.* 2012. http://heliosvoting.org/about-us/ (accessed November 5, 2012).

Al-Ameen, A., and S.A. Talab. "E-voting systems vulnerabilities." Jeju, South Korea: 8th International Conference on Information Science and Digital Content Technology (ICIDT), 2012.

Al-Shammari, A.F.N., A. Villafiorita, and K. Weldemariam. "Understanding the Development Trends of Electronic Voting Systems." Prague, Czech Republic: Seventh International Conference on Availability, Reliability and Security (ARES), 2012.

Alvarez, R. Michael, and Jonathan Nagler. "The Likely Consequences of Internet Voting for Political Representation." *Loyola of Los Angeles Law Review* 4, no. 1 (2001): 1115-1153.

Alvarez, R. Michael, and Thad E. Hall. *Electronic Elections.* Princeton NJ: Princeton University Press, 2008.

—. *Point, Click, and Vote: The Future of Internet Voting.* Washington, DC: Brookings Institute Press, 2004.

Alvarez, R. Michael, Stephen Ansolabehere, Thad E. Hall, Jonathan N. Katz, Ronald L. Rivest, and Charles III Stewart. *Voting: What Has Changed, What Hasn't & What Needs Improvement.* Caltech/MIT Voting Technology Project, 2012.

Ansari, Nirwan, Pitipatana Sakarindr, Ehsan Haghani, Chao Zhang, Aridaman K. Jain, and Yun Q. Shi. "Evaluating electronic voting systems equipped with voter-verified paper records." *IEEE Security & Privacy* 6, no. 3 (2008): 30-39.

Appel, Andrew W. *Ceci n'est pas une urne: On the Internet vote for the Assembl´ee des Francais de l'etranger.* Rocquencourt, France: Princeton University, 2006.

—. "Effective audit policy for voter-verified paper ballots." Chicago: Annual Meeting of the American Political Science Association, 2007.

Appel, Andrew W. "Security Seals on Voting Machines A Case Study." *ACM Transactions on Information and System Security* 14, no. 2 (2011).

Appel, Andrew W., et al. *The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine.* Montreal, Canada: Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, 2009.

Appel, Andrew W., Maia Ginsburg, Harri Hursti, Brian W. Kernighan, Christopher D. Richards, and Gang Tan. *Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine.* Princeton, NJ: Princeton University, 2008.

Arnold, Edward G. *History of Voting Systems in California.* Sacramento, CA: Secretary of State of California, 1999.

Ash, Arlene, and John Lamperti. "Florida's District 13 Election in 2006: Can Statistics Tell Us Who Won?" *Chance* 21 (2008): 2-10.

Ashkenas, Jeremy, Matthew Ericson, Alicia Parlapiano, and Derek Willis. "The 2012 Money Race: Compare the Candidates." *New York Times.* 2012. http://elections.nytimes.com/2012/campaign-finance (accessed December 5, 2012).

—. *The 2012 Money Race: Compare the Candidates.* 2012. http://elections.nytimes.com/2012/campaign-finance (accessed December 5, 2012).

Associated Press. "3 more Iowa election fraud cases are filed." *Omaha.com.* November 22, 2012. http://www.omaha.com/article/20121122/NEWS/121129921/1707 (accessed December 24, 2012).

—. "Fewer blind Americans learning to use Braille: Less than 10 percent of 1.3 million legally blind can read the raised dots." *NBC News.* March 26, 2009. http://www.nbcnews.com/id/29882719/#.UTKQTTD_mSo (accessed March 2, 2013).

—. "Voter turnout 2012: Voters in N.Y., N.J. not deterred by storm's effects." *Politico.* November 6, 2012. http://www.politico.com/news/stories/1112/83408.html (accessed November 6, 2012).

Aviv, Adam, et al. "Security Evaluation of ES&S Voting Machines and Election Management System." San Jose, CA: USENIX/ACCURATE Electronic Voting Technology Workshop, 2008.

Baxter, Christopher, and Statehouse Bureau. "N.J. sees record-low voter turnout in wake of Hurricane Sandy." *NewJersey.com.* November 7, 2012. http://www.nj.com/politics/index.ssf/2012/11/nj_sees_record-low_voter_turno.html (accessed November 8, 2012).

Beard, Charles. *An Economic Interpretation of the Constitution of the United States.* New Brunswick, New Jersey: Transaction Publishers, 2002.

Bhalla, Jonathan. "Can tech revolutionize African elections?" *CNN.* November 17, 2012. http://www.cnn.com/2012/11/17/opinion/sierra-leone-election-biometric/index.html (accessed November 17, 2012).

Blade Columbus Bureau. "Governor OKs law requiring paper trail for new vote devices." *Toledo Blade.* May 8, 2004. http://www.toledoblade.com/State/2004/05/08/Governor-OKs-law-requiring-paper-trail-for-new-vote-devices.html (accessed December 8, 2012).

Booth, Darren. "Ryanair's Outrageous Boarding Pass Fee: US Airlines Next?" *CNBC.* August 24, 2012. http://www.cnbc.com/id/48765497/Ryanair_s_Outrageous_Boarding_Pass_Fee_US_Airlines_Next (accessed December 4, 2012).

Bryant, Randal E. *Computer Systems : Programmer's Perspectives - 2nd edition.* New York: Prentice Hall, 2010.

C., JoyBell C. "Quotable Quotes." *GoodReads.com.* 2013. http://www.goodreads.com/quotes/469248-choose-your-battles-wisely-after-all-life-isn-t-measured-by (accessed March 2, 2013).

Calandrino, Joseph A., Ariel J. Feldmen, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller. *Source Code Review of the Diebold Voting System.* Sacramento, CA: California Secretary of State "Top-to-Bottom" Review, 2007.

Calhoun, Pat. "The Terrorist Hack that Shocked America – and Why it Matters." *CNBC.* December 12, 2012. http://www.cnbc.com/id/100306578/The_Terrorist_Hack_that_Shocked_America_ndash_and_Why_it_Matters (accessed March 11, 2013).

Carter, Lemuria, and Ronald Campbell. "The Impact of Trust and Relative Advantage on Internet Voting Differences." *Journal of Theoretical and Applied Electronic COmmerce Research* 6, no. 3 (2010): 28-42.

Castro, Daniel. *Stop the Presses: How Paper Trails Fail to Secure e-Voting.* Washington, DC: The Information Technology & Innovation Foundation, 2007.

Chaum, David. "Secret-Ballot Receipts: True Voter-Verifiable Elections." *RSA Laboratories CryptoBytes* 7, no. 2 (2004): 13-26.

Chen, David W. "City Finally Poised to Give Up Lever Voting Machines." *New York Times.* January 3, 2010. http://www.nytimes.com/2010/01/04/nyregion/04machines.html?_r=0 (accessed November 10, 2012).

Claassen, Ryan L., David B. Magleby, J. Quin Monson, and Kelly D. Patterson. "Voter Confidence and the Election-Day Voting Experience." *Political Behavior*, 2012.

Clark County Nevada. *Clark County Nevada Elecitons.* 2013. http://www.clarkcountynv.gov/Depts/election/ (accessed February 14, 2013).

Clark, Jeremy, and Urs Hengartner. "Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance." St. Lucia: Financial Cryptography and Data Security, 2011.

Clarkson, Michael, Brian Hay, Meador Inge, Abhi Shelat, David Wagner, and Alec Yasinsac. "Software Review and Security Analysis of Scytl Remote Voting Software." Tallahassee, FL: Department of State, Florida, 2009.

Clayton, Mark. "Could e-voting machines in Election 2012 be hacked? Yes." *Christian Science Monitor.* October 26, 2012. http://www.csmonitor.com/USA/Elections/2012/1026/Could-e-voting-machines-in-Election-2012-be-hacked-Yes (accessed October 27, 2012).

Cline, Seth. "12 Biggest Donors of the 2012 Election." *US News.* October 26, 2012. http://www.usnews.com/news/articles/2012/10/26/12-biggest-donors-of-the-2012-election (accessed February 3, 2013).

CNN. "CNN Election 2012: Results." *CNN.* December 10, 2012. http://www.cnn.com/election/2012/results/main (accessed February 20, 2013).

Cohen, Adam. "The Good News (Really) About Voting Machines." *New York Times.* January 10, 2007. http://www.nytimes.com/2007/01/10/opinion/11talkingpoints.html?pagewanted=all&_r=0 (accessed December 4, 2012).

Cohen, Andrew. "Think the Florida Recount Was Bad? Just Wait Until November 6." *The Atlantic.* October 22, 2012. http://www.theatlantic.com/politics/archive/2012/10/think-the-florida-recount-was-bad-just-wait-until-november-6/263901/ (accessed October 30, 2012).

Coney, Lillie, Joseph L. Hall, Poorvi L. Vora, and David Wagner. "Towards a Privacy Measurement Criterion for Voting Systems." Atlanta: National Conference on Digital Government Research, 2005.

Connors, Bob, LeAnne Gendreau, and Jeff Saperstone. "Court Hearing, Extended Voting Hours Over Bridgeport Ballots." *NBC CT.* November 2, 2010. http://www.nbcconnecticut.com/news/politics/Polls-Running-Low-on-Ballots-106559278.html (accessed December 30, 2012).

Cordero, Ariel, and David Wagner. "Replayable Voting Machine Audit Logs." San Jose, CA: Electronic Voting Technology Workshop, 2008.

Cowan, Sarah K., Stephen Doyle, and Drew Heffron. "How Much Is Your Vote Worth?" *New York Times.* November 1, 2008. http://www.nytimes.com/2008/11/02/opinion/02cowan.html?_r=1& (accessed Novemebr 8, 2012).

—. "How Much Is Your Vote Worth?" November 1, 2008. http://www.nytimes.com/2008/11/02/opinion/02cowan.html?_r=1& (accessed Novemebr 8, 2012).

Damron, Gina, and Christina Hall. "Voter turnout high across metro Detroit, despite hours-long lines at many places." *Detroit Free Press.* November 6, 2012. http://www.freep.com/article/20121106/NEWS15/121106074/voter-turnout-metro-detroit (accessed November 6, 2012).

Dewdney, A.K. "Computer Recreations: Of Worms, Viruses and Core War." *Scientific American*, March 1989: 110.

Dicken, Brad. "Henrietta Township man accused of voting twice." *North Coast Chronicle.* November 21, 2012. http://chronicle.northcoastnow.com/2012/11/21/henrietta-township-man-accused-of-voting-twice/ (accessed December 24, 2012).

Doig, Matthew, and Maurice Tamman. "Analysis suggests undervote caused by ballot design." *Herald-Tribune.* November 15, 2006. http://www.heraldtribune.com/apps/pbcs.dll/article?p=5&tc=pg&AID=/20061115/NEWS/611150751 (accessed December 23, 2012).

Edwards, Johnny. "State investigators: Fulton election documents were altered." *The Atlanta Journal-Constitution.* January 31, 2013. http://www.ajc.com/news/news/state-regional-govt-politics/state-investigators-fulton-election-documents-were/nWCQw/ (accessed February 15, 2013).

Elliott, Scott. *ElectionProjection.com.* 2012. http://www.electionprojection.com (accessed Februay 1, 2012).

Engleman, Eric. "Security of N.J. E-Mail Voting After Storm Is Questioned." *Bloomberg Businessweek.* November 6, 2012. http://www.businessweek.com/news/2012-11-06/security-of-n-dot-j-dot-e-mail-voting-after-storm-is-questioned (accessed November 7, 2012).

Epstein, Jeremy, Joseph Lorenzo Hall, Walter Mebane, Alex Halderman, and Susan Dzieduszycka-Suinat. "Comments During Panel Presentation." Online: Princteon CITP E-voting Workshop, 2012.

Estehghari, Saghar, and Yvo Desmedt. "Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example." Washington, DC: Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, 2010.

Esteve, Jordi Barrat i, Ben Goldsmith, and John Turner. *International Experience with E-Voting.* Washington, DC: International Foundation for Electoral Studies, 2012.

Evans, Eldon Cobb. *A history of the Australian ballot system in the United States.* Chicago: University of Chicago Press, 1917.

Everett, Sarah P. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection.* Houston, TX: Rice University, 2007.

Everett, Sarah P., et al. "Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance." Florence, Italy: CHI 2008 Proceedings: Measuring, Business, and Voting, 2008.

Exner, Rich. "Ohio voter registration and 2012 turnout by county." *Cleveland.com.* November 15, 2012. http://www.cleveland.com/datacentral/index.ssf/2012/11/ohio_voting_registration_and_2.html (accessed February 2, 2013).

Fairfax County Virginia. "Commonwealth of Viriginia County of Fairfax 2012 Districts, Precincts & Polling Places." *Fairfax County Virginia.* September 1, 2012. http://www.fairfaxcounty.gov/elections/pcts/1aa2012directoryofdistrictsprecinctsandpollingplacesrevsept2012.pdf (accessed February 16, 2013).

FairVote. *Faithless Electors.* 2005. http://archive.fairvote.org/e_college/faithless.htm (accessed November 8, 2012).

Federal Election Commission. "2000 Official Presidential General Election Results." *Federal Election Commission.* December 2001. http://www.fec.gov/pubrec/2000presgeresults.htm (accessed December 25, 2012).

Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten. "Security Analysis of the Diebold AccuVote-TS Voting Machine." Boston: Electronic Voting Technology Workshop, 2007.

Fineout, Gary. "Florida finds evidence of voter registration fraud." *Miami Herald.* March 5, 2013. http://www.miamiherald.com/2013/03/05/3268426/florida-finds-evidence-of-voter.html (accessed March 12, 2013).

Foley, John P. Ed. *The Jeffersonian Cyclopedia.* New York: Funk & Wagnalls Company, 1900.

Frisina, Laurin, Michael C. Herron, James Honaker, and Jeffrey B. Lewis. "Ballot formats, touchscreens, and undervotes: A study of the 2006 midterm elections in Florida." *Election Law Journal* 7, no. 1 (2008): 25-47.

Gainey, David, Michael Gerke, and Alec Yasinsac. *Software Review and Security Analysis of the Diebold Voting Machine Software Supplemental Report.* Tallahassee: Office of the Secretary of State of Florida, 2007.

Gallup. "U.S. Presidential Election Center." *Gallup.* 2012. http://www.gallup.com/poll/154559/US-Presidential-Election-Center.aspx?ref=interactive (accessed February 2, 2013).

Gambino, Megan. "We Can Bank Online. Why Can't We Vote Online?" *Smithsonian Institute.* November 6, 2012. http://blogs.smithsonianmag.com/ideas/2012/11/we-can-bank-online-why-cant-we-vote-online/ (accessed November 9, 2012).

Garber, Kitty. *Lost Votes in Florida's 2006 General Election: A Look at Extraordinary Undervote Rates On the ES&S iVotronic.* Tallahassee, FL: Florida Fair Elections Center, 2007.

Gardner, Aaron. "Colorado Counties Have More Voters Than People." *Red State.* September 4, 2012. http://www.redstate.com/2012/09/04/colorado-counties-have-more-voters-than-people/ (accessed September 8, 2012).

Garfinkle, Norton, and Patrick Glynn. *Report on Election Systems Reform.* Washington, DC: Institute for Communitarian Policy Studes: The George Washington University, 2001.

Geanakopolos, John. "Three Breif Proofs of Arrow's Impossibility Theorem." *Economic Theory* 26 (2005): 211-215.

Ghosh, Anup, and Gary McGraw. "Lost Decade or Golden Era: Computer Security since 9/11." *Security & Privacy, IEEE* 10, no. 1 (2012): 6-10.

Goffard, Christopher, and Rosanna Xia. "O.C. voter turnout far behind 2008, but mail-in ballots up." *Los Angeles Times.* November 6, 2012. http://latimesblogs.latimes.com/lanow/2012/11/oc-voter-turnout-lower-than-2008-so-far.html (accessed November 7, 2012).

Goodman, Susannah, Michelle Mulder, and Pamela Smith. *Counting Votes 2012: A State by State Look at Voting Technology Preparedness.* Rutgers, NJ: Verified Voting, Common Cause and the Rutgers School of Law, 2012.

Google Maps. *Google Maps.* February 18, 2013. http://maps.google.com (accessed February 18, 2013).

Gore, Al. "Gore: Let's make sure this time every vote is counted." July 6, 2004. http://articles.cnn.com/2004-07-26/politics/dems.gore.transcript_1_vote-counts-republican-challenges-popular-vote?_s=PM:ALLPOLITICS (accessed February 15, 2013).

Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *The Wall Street Journal.* April 21, 2009. http://online.wsj.com/article/SB124027491029837401.html (accessed January 24, 2013).

Government Accountability Board: State of Wisconsin. "State of Wisconsin Registered Voters by Municipality Within County." *Government Accountability Board: State of Wisconsin.* November 2, 2012. http://gab.wi.gov/sites/default/files/publication/65/registeredvotersbymunicipality_pdf_11336.pdf (accessed February 1, 2013).

—. "Voting Equipment." *Government Accountability Board: State of Wisconsin.* April 21, 2010. http://gab.wi.gov/sites/default/files/page/voting_equipment_by_municipality_2_pdf_15114.pdf (accessed February 1, 2013).

Greene, K. Kristen. *Usability of New Electronic Voting Systems and Traditional Methods: Comparisons Between Sequential and Direct Access Electronic Voting Interfaces, Paper Ballots, Punch Cards, and Lever Machines.* Houston, TX: Rice University, 2008.

Gumbel, Andrew. *Steal This Vote.* New York: Nation Books, 2005.

H.R. 12. (2013).

Halderman, J. Alex, Eric Rescorla, Hovav Shacham, and David Wagner. "You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems." San Jose, CA: Electronic Voting Workshop, 2008.

Hamilton, Alexander. "Transcript of Federalist Papers, No. 10 & No. 51 (1787-1788)." *OurDocuments.gov.* n.d. http://www.ourdocuments.gov/doc.php?flash=true&doc=10&page=transcript (accessed Novemeber 12, 2012).

Hansen, Richard L. *The Voting Wars.* New Haven, CT: Yale University Press, 2012.

Helms, Jesse. "Quotes." 2013. http://www.brainyquote.com/quotes/quotes/j/jessehelms275811.html (accessed February 15, 2013).

Herrnson, Paul. *Voting Technology: the not so simple act of casting a ballot.* Washington DC: Brookings Institute Press, 2008.

Herron, Michael C., and Daniel A. Smith. "High ballot rejection rates should worry Florida voters." *Tampa Bay Times.* October 28, 2012. http://www.tampabay.com/opinion/columns/high-ballot-rejection-rates-should-worry-florida-voters/1258477 (accessed February 2, 2013).

Hickins, Michael. "The Morning Download: Cracking Banks and Hacking Votes." *The Wall Street Journal CIO Report.* September 27, 2012. http://blogs.wsj.com/cio/2012/09/27/the-morning-download-cracking-banks-and-hacking-votes/?mod=djemCIO_h (accessed September 30, 2012).

Hobbes, Thomas. *Leviathan: a critical edition by G.A.J. Rogers and Karl Schuhman.* Briston, England: Thoemmes Continuum, 2003.

Holbrook, Stett. "How to Hack an Election: A Cautionary Tale." *Makezine.com.* November 5, 2012. http://blog.makezine.com/2012/11/05/how-to-hack-an-election-a-cautionary-tale/ (accessed November 6, 2012).

Hoover, J. Nicholas. "Election 2012: New Voting Tech Caused Some Headaches." *Information Week.* November 7, 2012. http://www.informationweek.com/government/information-management/election-2012-new-voting-tech-caused-som/240062512 (accessed November 8, 2012).

Howard, Greyson, and Ryan Slabaugh. "Power outage only reported issue on election day: Outage did not affect voters; paper ballots used in Glenshire." *Sierra Sun.* November 4, 2008. http://www.sierrasun.com/article/20081104/NEWS/811049949 (accessed January 23, 2013).

Howington, James Richard. "Harry S. Truman Quote's Page." 2013. http://scmidnightflyer.com/truman.html (accessed February 18, 2013).

IBM. "Votomatic." *IBM.* n.d. http://www-03.ibm.com/ibm/history/exhibits/supplies/supplies_5404PH12.html (accessed November 22, 2012).

Irish Times Editors. "Rogue voting machine switches sides." *Irish Times.* November 7, 2012. http://www.irishtimes.com/newspaper/breaking/2012/1107/breaking6.html (accessed November 8, 2012).

James, Scott. "Despite the Fanfare, Little Proof of Election Irregularities." *New York Times.* November 10, 2011. http://www.nytimes.com/2011/11/11/us/despite-the-fanfare-little-proof-of-election-irregularities.html (accessed November 17, 2012).

Jauregui, Andres. "Pennsylvania Voting Machine Switches Vote From Barack Obama To Mitt Romney (VIDEO)." *Huffington Post.* November 6, 2012. http://www.huffingtonpost.com/2012/11/06/pennsylvania-voting-machine-switches-vote-obama-romney_n_2083015.html (accessed November 6, 2012).

Jefferson, David, Aviel D. Rubin, Barbara Simons, and David Wagner. *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).* Pentagon City, VA: United States Department of Defense, 2004.

Jefferson, David, Aviel D. Rubin, Barbara Simons, and David Wagner. "Analyzign Internet Voting Security." *Communications of the ACM* 47, no. 10 (2004): 59-64.

Johnston, Roger. "How I Hacked An Electronic Voting Machine." *Popular Science.* November 5, 2012. http://www.popsci.com/gadgets/article/2012-11/how-i-hacked-electronic-voting-machine (accessed March 1, 2013).

Jones, Douglas W. "Computer Security Versus the Public's Right to Know." Montreal: Electronic Voting Integrity, 2007.

Jones, Douglas W. "Misassessment of Security in Computer-Based Election Systems." *RSA Laboratories CryptoBytes* 7, no. 4 (2004): 8-12.

Jones, Douglas W. "On Optical Mark-Sense Scanning." In *Towards Trustworthy Elections*, by David Ed. Chaum, 175-190. Berlin: Springer, 2010.

—. "Sarasota Panel: Vote-o-graph results from Iowa." San Francisco: Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, 2011.

—. "Technologists as Political Reformers: Lessons from the Early History of Voting Machines." Las Vegas, NV: Society for the History of Technology Annual Meeting, 2006.

—. "Threats to Voting Systems." Gaithersburg, MD: Workshop on Developing an Analysis of Threats to Voting Systems, 2005.

—. "Voting Security A Technical Perspective." Columbia, SC: University of South Carolina Cybersecurity Symposium, 2005.

Josh. "Self Deleting Prank Virus!" *YouTube.* June 3, 2007. http://www.youtube.com/watch?v=jlCyYFJSEGo (accessed December 20, 2012).

Karlof, Chris, Naveen Sastry, and David Wagner. "Cryptographic Voting Protocols: A Systems Perspective." Anaheim, CA: USENIX, 2005.

Karlof, Chris, Naveen Sastry, and David Wagner. *The Promise of Cryptographic Voting Protocols.* Berkeley, CA: University of California at Berkeley, 2005.

Keller, Arthur M., David Mertz, Joseph Lorenzo Hall, and Arnold Urken. "Privacy Issues in an Electronic Voting Machine." New York: Proceedings of the 2004 ACM workshop on Privacy in the electronic society, 2004.

Kerski, John. *Electronic Voting: Trusted Removeable Media and Its Contents.* Tallahassee, FL: Florida State University, 2008.

Kiayias, A., et al. "Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting." Miami: Computer Security Applications Conference, 2008.

Kiayias, A., L. Michael, A. Russell, and A. A. Shvartsman. *Integrity Vulnerabilities in the Diebold TSX Voting Terminal.* Stores, CT: UConn Voting Technology Research Center, 2007.

Killian, Johnny H. "Constitution of the United States." *United States Senate.* n.d. http://www.senate.gov/civics/constitution_item/constitution.htm (accessed November 23, 2012).

Kingkade, Tyler. "Youth Vote 2012 Turnout: Exit Polls Show Greater Share Of Electorate Than In 2008." *Huffington Post.* November 7, 2012. http://www.huffingtonpost.com/2012/11/07/youth-vote-2012-turnout-exit-polls_n_2086092.html (accessed November 7, 2012).

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. "Analysis of Electronic Voting Machines." Berkeley, CA: IEEE Symposium on Security and Privacy, 2004.

Kremer, Steve, Mark D. Ryan, and Ben Smyth. "Election verifiability in electronic voting protocols." Athens: Proceedings of the 15th European Symposium on Research in Computer Security, 2012.

Krugman, Paul. "Hack The Vote." *New York Times.* December 2, 2003. http://www.nytimes.com/2003/12/02/opinion/hack-the-vote.html (accessed November 7, 2012).

Kumar, D.A., and T. U. S. Begum. "Electronic voting machine — A review." Tamilnadu, India: International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME) , 2012.

Kusters, R., T. Truderung, and A. Vogt. "Clash Attacks on the Verifiability of E-Voting Systems." San Fransisco: IEEE Symposium on Security and Privacy, 2012.

Kwak, Haewoon, Changhyun Lee, Hosung Park, and Sue Moon. "What is Twitter, a Social Network or a News Media?" Raleigh, NC: International World Wide Web Conference Committee, 2010.

League of Women Voters of Texas. "Voter Information." *League of Women Voters of Texas.* 2012. http://lwvtexas.org/votersintro.php (accessed December 25, 2012).

Lee, Jennifer. "A Love Affair With Lever Voting Machines." *New York Times.* March 10, 2009. http://cityroom.blogs.nytimes.com/2009/03/10/a-love-affair-with-lever-voting-machines/ (accessed November 25, 2012).

Levine, Art. "Ohio, Facing Vote-Rigging Lawsuit, Adds Voter-Purging Software: Are Dems, Liberals, Election Officials Ready to Safeguard Votes?" *Huffington Post.* November 2, 2012. http://www.huffingtonpost.com/art-levine/mia-in-voting-machine-war_b_2054411.html (accessed February 3, 2013).

Limbaugh, Rush. "Pearls of Wisdom." *Rush Limbaugh.* September 10, 2012. http://www.rushlimbaugh.com/daily/2012/09/10/pearls_of_wisdom (accessed January 24, 2013).

Lindeman, Mark, Mark Halvorson, Pamela Smith, Lynn Garland, Vittorio Addona, and Dan McCrea. *Principles and Best Practices for Post-Election Audits.* ElectionAudits.org, 2008.

Liptak, Adam. "Error and Fraud at Issue as Absentee Voting Rises." *New York Times.* October 6, 2012. http://www.nytimes.com/2012/10/07/us/politics/as-more-vote-by-mail-faulty-ballots-could-impact-elections.html?pagewanted=all (accessed October 7, 2012).

—. "Voting Rights Law Draws Skepticism From Justices." *New York Times.* February 27, 2013. http://www.nytimes.com/2013/02/28/us/politics/conservative-justices-voice-skepticism-on-voting-law.html?hp&_r=1& (accessed February 27, 2013).

Liss, Josh. "2012 Primary mail ballot election information." *Jefferson County Colorado.* May 24, 2012. http://jeffco.us/jeffco/elections_uploads/PDF_News_Release___Primary_Primer_5_24_12.pdf (accessed February 17, 2013).

Logan, Dean C. *King Country Elections Moving To Vote By Mail.* Seattle, WA: King Country Elections, 2006.

Lucas, George. "Indiana Jones and the Last Crusade." *Wikiquote.* 2013. http://en.wikiquote.org/wiki/Indiana_Jones_and_the_Last_Crusade (accessed March 12, 2013).

Luckovich, Mike. "Political Humor: Voting Technology." *Mike Luckovich.* November 17, 2012. http://blogs.ajc.com/mike-luckovich/page/8/ (accessed February 28, 2013).

Manning, Stephen. "Paper Jams Hamper Electronic Voting." *Washington Post.* December 26, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/12/21/AR2006122100123.html (accessed October 7, 2012).

Mapes, Jeff. "Ballot fraud allegations in Clackamas County could lead to changes in election procedures." *The Oregonian.* November 10, 2012. http://www.oregonlive.com/politics/index.ssf/2012/11/ballot_fraud_allegations_in_cl.html (accessed November 10, 2012).

Margo, Robert A. *Race and Schooling in the South: A Review of the Evidence.* Chicago: University of Chicago Press, 1990.

Mascher, Andrea L., Paul T. Cotton, and Douglas W. Jones. "Improving Voting System Event Logs." Atlanta: First International Workshop on Requirements Engineering for E-voting Systems, 2009.

Mazzei, Patricia. "The case of the phantom ballots: an electoral whodunit." *Miami Herald.* February 23, 2013. http://www.miamiherald.com/2013/02/23/3250726/the-case-of-the-phantom-ballots.html#storylink=misearch (accessed March 1, 2013).

McConnell, Steve. *Code Complete 2.* Cambridge, MA: O'Rilley, 2004.

McDaniel, Patrick, Matt Blaze, Giovanni Vigna, Joseph Lorenzo Hall, Laura Quilter, and Various. *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing.* Columbus, OH: Ohio Secretary of State: EVEREST Project, 2007.

McNeece, Joel. "Vardaman Town Hall Broken Into." *Calhoun County Journal.* August 10, 2009. http://www.calhouncountyjournal.com/vardaman-town-hall-broken-into/ (accessed February 2, 2013).

Mears, Bill. "Provisional ballots could be key if Ohio margin razor thin." November 5, 2012. http://www.cnn.com/2012/11/05/politics/ohio-ballots/index.html (accessed February 2, 2013).

Mebane, Walter R. Jr. "Revisited, Machine Errors and Undervotes in Florida 2006." New Orleans, LA: Convention of the Southern Political Science Association, 2009.

Mebane, Walter R. Jr. "The Wrong Man is President! Overvotes in the 2000 Presidential Eleciton in Florida." *Symposium: U.S. Elecitons* 2, no. 3 (2004): 525-535.

Mebane, Walter R. Jr., and David L. Dill. *Factors Associated with the Excessive CD-13 Undervote in the 2006 General Election in Sarasota County, Florida.* Tallahassee, FL: Florida State University, 2007.

Mello, Suzanne Irene. *A Detailed Forensic Analysis and Recommendations For Rhode Island's Present and Future Voting Systems.* Providence, RI: University of Rhode Island Department of Computer Science, 2011.

Mercuri, Rebecca. "Voting-Machine Risks." *Communications of the ACM* 35, no. 11 (1992): 138.

Metasploit. *Metasploit.* 2012. http://www.metasploit.com/ (accessed January 16, 2013).

Microsoft. "10 Immutable Laws of Security." *Microsoft.* 2012. http://technet.microsoft.com/library/cc722487.aspx (accessed February 2, 2013).

Miller, Geralyn M. *Changing the Way America Votes.* Lewiston NY: Edwin Mellen Press, 2004.

Miller, Stephen. "Electronic Voting Machines Add Uncertainty to Close Election Race." *CorpWatch.org.* September 8, 2004. http://www.corpwatch.org/article.php?id=11518 (accessed November 17, 2012).

Molnar, David, Tadayoshi Kohno, Naveen Sastry, and David Wagner. "Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract)." Oakland, CA: IEEE Symposium on Security and Privacy, 2006.

Morrell, Dan. "Secret Ballots, Verifiable Votes." *Harvard Magazine.* May-June 2012. http://harvardmagazine.com/2010/05/secret-ballots-verifiable-votes?page=0,1 (accessed December 11, 2012).

Mother Jones News Team. "Full Transcript of the Mitt Romney Secret Video." *Mother Jones.* September 19, 2012. http://www.motherjones.com/politics/2012/09/full-transcript-mitt-romney-secret-video (accessed February 18, 2013).

National Archives. "Declaration of Independence." *National Archives.* 2012. http://www.archives.gov/exhibits/charters/declaration_transcript.html (accessed January 23, 2013).

National Federation of the Blind. "The Blind and Visually Impaired Voter's Guide." 2012. https://nfb.org/blind-voters-guide (accessed December 25, 2012).

New York Times. "New York Times 2008 Election Center." *New York Times.* December 9, 2008. http://elections.nytimes.com/2008/index.html (accessed February 14, 2013).

Norden, Lawrence. *Issue Brief: Election 2012 Recounts.* New York: Brennan Center For Justice, 2012.

Norden, Lawrence. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost.* New York: Brennan Center For Justice at New York University School of Law, 2006.

Norden, Lawrence. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost.* New York: Brennan Center For Justice at New York University School of Law, 2006.

Norden, Lawrence. *Voting System Failures: A Database Solution.* New York: Brennan Center for Justice at New York University School of Law, 2010.

Norden, Lawrence, Aaron Burstein, Joseph Lorenzo Hall, and Margaret Chen. *Post Election Audits: Restoring Trust in Elections.* New York: Brennan Center For Justice at New York University School of Law, 2007.

Norden, Lawrence, et al. *The Machinery of Democracy: Protecting Elections in an Electronic World.* New York: Brennan Center For Justice at New York University School of Law, 2006.

Norden, Lawrence, Whitney Quesenbery, and David C. Kimball. *Better Design, Better Elections.* New York: Brennan Center For Justice at New York University School of Law, 2012.

Office of the Secretary of State of California. "Voter Registration Form." *Office of the Secretary of State of California.* 2012. https://rtv.sos.ca.gov/elections/register-to-vote/?AspxAutoDetectCookieSupport=1 (accessed December 4, 2012).

Office of the Secretary of State of Georgia. "Georgia Voter Identification Requirements." *Office of the Secretary of State of Georgia.* 2012. http://www.sos.georgia.gov/gaphotoid/default.htm (accessed December 25, 2012).

Office of the Secretary of State of Minnessota. "2008 U.S. Senate Race." *Office of the Secretary of State of Minnessota.* 2009. http://www.sos.state.mn.us/index.aspx?page=1405 (accessed December 25, 2012).

Office of the Secretary of State of Nevada. "2008 Official Statewide General Election Results: Voter Turnout Report." *Office of the Secretary of State of Nevada.* 2009. http://nvsos.gov/SOSelectionPages/results/2008StateWideGeneral/VoterTurnout.aspx (accessed February 12, 2013).

Office of the Secretary of State of Ohio. "2008 Ohio Election Calendar." *Office of the Secretary of State of Ohio.* October 2007. http://vote.franklincountyohio.gov/assets/pdf/2008/electionCalendar2008.pdf (accessed February 2, 2013).

—. "2012 Ohio Election Calendar." *Office of the Secretary of State of Ohio.* December 14, 2011. http://www.sos.state.oh.us/sos/upload/publications/election/2012ElectionCalendar_11x17.pdf (accessed February 2, 2013).

—. "Voter Files Download Page." *Office of the Secretary of State of Ohio.* January 27, 2013. http://www2.sos.state.oh.us/pls/voter/f?p=111:1 (accessed February 2, 2013).

—. "Voter Turnout: November 4, 2008." *Office of the Secretary of State of Ohio.* 2009. http://www.sos.state.oh.us/sos/elections/Research/electResultsMain/2008ElectionResults/turnout110408.aspx (accessed February 12, 2013).

Office of the Secretary of State of Washington. "2004 Governor's Race." *Office of the Secretary of State of Washington.* 2005. http://www.sos.wa.gov/elections/2004gov_race.aspx (accessed December 25, 2012).

One, Aleph. "Smashing The Stack For Fun And Profit." *Wright University.* November 8, 1996. http://www.cs.wright.edu/people/faculty/tkprasad/courses/cs781/alephOne.html (accessed January 24, 2013).

Orlando, Jennifer Darwin. *Accountability of Electronic Voting Systems in Florida: An Analysis of Policy Options.* Tallahassee, FL: Florida State University, 2005.

Orol, Ronald D. "Voters turn out in rain, heat and cold for Obama vs. Romney election." *MarketWatch.* November 6, 2012. http://blogs.marketwatch.com/election/2012/11/06/voters-turn-out-in-rain-heat-and-cold-for-obama-vs-romney-election/ (accessed November 6, 2012).

Overton, Spencer. *Stealing Democaracy.* New York: W.W. Norton & Company Inc., 2006.

Percy, Herma Ph.D. *Will Your Vote Count?* Westport, CT: Praeger, 2009.

Perlroth, Nicole. "Hackers Step Up Attacks After Megaupload Shutdown." *New York Times.* January 24, 2012. http://bits.blogs.nytimes.com/2012/01/24/hackers-step-up-attacks-after-megaupload-shutdown/ (accessed December 2, 2012).

Pieters, W., and M.J. Becker. "Ethics of evoting: An essay on requirements and values in internet voting." Enschede, Netherlands: Proceedings of the Sixth International Conference of Computer Ethics, 2005.

Plancher, Brian, and Alana Pradhan. *IPSnail: A Hybrid Internet-Mail Voting System.* Cambridge, MA: Harvard Univeristy, 2012.

Plummer, Brad. "Estonia gets to vote online. Why can't America?" *Washington Post.* November 6, 2012. http://www.washingtonpost.com/blogs/wonkblog/wp/2012/11/06/estonians-get-to-vote-online-why-cant-america/ (accessed November 7, 2012).

—. "Five ways to make long elections lines shorter." *Washington Post.* November 8, 2012. http://www.washingtonpost.com/blogs/wonkblog/wp/2012/11/08/five-ways-to-cut-long-election-lines/ (accessed November 9, 2012).

Politico. "2012 Swing States." *Politico.* 2012. http://www.politico.com/2012-election/swing-state/ (accessed February 1, 2013).

Poundstone, William. *Gaming the Vote.* New York: Hill and Wang, 2008.

Purtill, Yvette. "Will Thousands of Military Ballots Not be Counted?" *Naval Enlisted Reserve Organization.* November 6, 2012. http://www.nera.org/index.php?option=com_content&view=article&id=191:military-ballots-not-counted&catid=81:blog1&Itemid=148 (accessed November 7, 2012).

Registrar of Voters Association of Connecticut. "Moderator's Handbook: For Marksense Voting Machines (Accu-Vote ES-2000)." *Registrar of Voters Association of Connecticut.* 2011. http://www.rovac.org/Moderator_Handbook_SOTS_2011.doc (accessed January 15, 2013).

Rezende, Pedro A. D. "Electronic Voting Systems Is Brazil ahead of its time?" *RSA Laboratories CryptoBytes* 7, no. 2 (2004): 1-5.

Rivest, Ron. "On the notion of 'software independence' in voting systems." *Philosophical Transactions of the Royal Society A*, August 6, 2008: 3759-3767.

Rivest, Ron. *Thoughts On Appropriate Technologies For Voting.* Online: Princteon CITP E-voting Workshop, 2012.

Rubin, Aviel D. PhD. *Brave New Ballot.* New York: Morgan Road Books, 2006.

Rubin, Jennifer. "Denver debate: A dominating night for Romney." *Washington Post.* October 3, 2012. http://www.washingtonpost.com/blogs/right-turn/post/denver-debate-a-dominating-night-for-romney/2012/10/03/b930ab1a-0da5-11e2-bd1a-b868e65d57eb_blog.html (accessed February 18, 2013).

Sastry, Naveen, Tadayoshi Kohno, and David Wagner. "Designing Voting Machines for Verification." Berkley, CA: Proceedings of the 15th conference on USENIX Security Symposium, 2006.

Schubarth, Cromwell. "Online elections can work, if there's a paper trail." *Silicon Valley Business Journal.* November 6, 2012. http://www.bizjournals.com/sanjose/blog/2012/11/online-elections-can-work-if-theres.html (accessed November 7, 2012).

SecurityBase.com. "Burglary by the Numbers." September 26, 2011. http://www.authoritysafes.com/burglary-statistics.html (accessed February 19, 2013).

Seitz, Justin. *Gray Hat Python: Python Programming for Hackers and Reverse Engineers.* San Francisco, CA: No Starch Press, 2009.

Sekler, Todd, and Jon Goler. *Security Vulnerabilities and Problems with VVPT.* Caltech/MIT Voting Technology Project, 2004.

Silver, Nate. "As Swing Districts Dwindle, Can a Divided House Stand?" *New York Times.* December 27, 2012. http://fivethirtyeight.blogs.nytimes.com/2012/12/27/as-swing-districts-dwindle-can-a-divided-house-stand/ (accessed December 28, 2012).

Smith. "Machines alter election votes: Hacking voting machines so easy that Grandma can do it." *Network World.* November 6, 2012. http://www.networkworld.com/community/blog/machines-alter-election-votes-hacking-voting-machines-so-easy-grandma-can-do-it (accessed November 7, 2012).

SOS Software. "Official Results: North Carolina 2008." *SOS Software.* March 17, 2010. http://results.enr.clarityelections.com/NC/7937/21334/en/vt_data.html (accessed February 12, 2013).

Spycher, O., and R. Haenni. "A novel protocol to allow revocation of votes a hybrid voting system." Johannesburg, South Africa: Information Security for South Africa (ISSA), 2010.

Stark, Phillip, and David Wagner. "Evidence Based Elections." *IEEE Security and Privacy* Special Issue on Electronic Voting (2012).

Stark, Phillip, Dan Wallach, Philip Kortum, David Wagner, and Edward W. Felten. "Comments During Panel Presentation." Online: Princteon CITP E-voting Workshop, 2012.

Stein, Perry. "Virginia's Sneaky Voter ID Raises Few Alarms." *The Republic.* November 6, 2012. http://www.tnr.com/blog/plank/109676/virginias-sneaky-voter-id-raises-few-alarms# (accessed December 25, 2012).

Stewart, Charles III. "A Data-Centered Look at the Election of 2008." Pasadena, CA: Technology, Diversity, and Democracy Symposium, 2009.

Stewart, Charles III. "Voting Technologies." *Annual Review of Political Science* 14 (2011): 353-378.

—. "What Hath HAVA Wrought?: Consequences, Intended and Not, of the Post-Bush v. Gore Reforms." Irvine, CA: Bush v. Gore, 10 Years Later: Election Administration in the United States, 2011.

Stewart, Charles III, R. Michael Alvarez, and Thad E. Hall. *Voting Technology and the Election Experience: The 2009 Gubernatorial Races in New Jersey and Virginia.* Caltech/MIT Voting Technology Project, 2010.

Stiner, Michelle Carfaro. "Anonymous claims Karl Rove tried to hack/steal the election (Video)." *Examiner.com.* November 18, 2012. http://www.examiner.com/article/anonymous-claims-karl-rove-tried-to-hack-steal-the-election (accessed November 18, 2012).

Stobo, J.R. *Organized Labor, Housing Issues, and Politics: Another Look at the 1886 Henry George Mayoral Campaign in New York City.* New York: Columbia University, 2008.

Streb, Matthew J. *Rethinking American Electoral Democracy.* New York: Routledge, 2008.

Sturton, Cynthia, Susmit Jha, Sanjit A. Seshia, and David Wagner. "On Voting Machine Design for Verification and Testability." Chicago: Conference on Computer and Communications Security, 2009.

Sunta, Stephanie. "Election officials still skeptical about online voting." *Northwestern University.* November 7, 2012. http://news.medill.northwestern.edu/chicago/news.aspx?id=210136 (accessed November 7, 2012).

SurfKY.com. "Grimes' Efforts to Prevent Vote Fraud Unanimously Passed by House." *SurfKY.com.* February 28, 2013. http://surfky.com/index.php/news/kentucky/27428-grimes-efforts-to-prevent-vote-fraud-unanimously-passed-by-house (accessed March 1, 2013).

Tarantino, Quentin. "Memorable Quotes from Django Unchained." *IMBD.* 2013. http://www.imdb.com/title/tt1853728/quotes (accessed February 18, 2013).

Taylor, Kate. "Chaos at City's Polls Amid New Voting Machines and Last-Minute Rules." *New York Times.* November 6, 2012. http://www.nytimes.com/2012/11/07/nyregion/chaos-at-new-york-city-polls-amid-new-rules-and-voting-machines.html?_r=0 (accessed November 9, 2012).

TechRadar. "How to avoid being captured on CCTV." *TechRadar.* January 21, 2008. http://www.techradar.com/us/news/world-of-tech/how-to-avoid-being-captured-on-cctv-244353 (accessed February 2, 2013).

Ted the Tool. "MIT Guide to Lock Picking." *Capricorn.org.* September 1, 1991. http://www.capricorn.org/~akira/home/lockpick/mitlg-a4.pdf (accessed February 2, 2013).

Tedeschi, Ernie. "In Defense of Electronic Voting Machines." *Policy Matters* 4, no. 1 (Autum 2006): 40-42.

Terry, Alllison. "Got broadband? Access now extends to 94 percent of Americans." *The Christian Science Monitor.* August 24, 2012. http://www.csmonitor.com/USA/Society/2012/0824/Got-broadband-Access-now-extends-to-94-percent-of-Americans (accessed December 4, 2012).

The Economist. "A really secret ballot." *The Economist.* October 22, 2008. http://www.economist.com/node/12455414 (accessed December 11, 2012).

Theisen, Ellen. "Ballot-Scanner Voting System Failures ." *VotersUnite.org.* May 22, 2009 . http://www.votersunite.org/info/opscansinthenews.pdf (accessed November 2, 2012).

Thompson, Clive. "Can You Count on Voting Machines?" *New York Times.* January 6, 2008. http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html?pagewanted=all&_r=0 (accessed November 3, 2012).

Thompson, Ken. "Reflextions on Trusting Trust." *Communication of the ACM* 27, no. 8 (1984).

Tolentino, Mellisa. "Election 2012: Hacking, Malfunctioning Machines, Bounced E-mails, and The Plea." *Silicon Angle.* November 7, 2012. http://siliconangle.com/blog/2012/11/07/election-2012-hacking-malfunctioning-machines-bounced-e-mails-and-the-plea/ (accessed November 8, 2012).

Trombley, William. "'Votomatic' Still Holds Lead Among Vote-Counting Systems." *Los Angeles Times.* July 2, 1989. http://articles.latimes.com/1989-07-02/news/mn-4899_1_vote-counting-system (accessed November 25, 2012).

TurboVote. *TurboVote.* 2012. https://turbovote.org (accessed December 25, 2012).

Tzu, Sun. "The Art of War: Chapter VI: Emptiness and Fullness." 2012. http://web.mit.edu/~dcltdw/AOW/6.html (accessed February 2, 2013).

U.S. Election Assistance Commission. *2004 Election Administration and Voting Survey.* Washington, D.C.: U.S. Election Assistance Commission, 2005.

U.S. Election Assistance Commission. *2006 Election Administration and Voting Survey.* Washington, D.C.: U.S. Election Assistance Commission, 2007.

U.S. Election Assistance Commission. *2008 Election Administration and Voting Survey.* Washington, D.C.: U.S. Election Assistance Commission, 2009.

U.S. Election Assistance Commission. *2010 Election Administration and Voting Survey.* Washington, D.C.: U.S. Election Assistance Commission, 2011.

U.S. Election Assistance Commission. *The Impact of the National Voter Registration Act of 1993 on the Administration of Elections for Federal Office 2007-2008.* Washington, D.C.: U.S. Election Assistance Commission, 2009.

Ungar, Rick. "Romney Family Investment Ties To Voting Machine Company That Could Decide The Election Causing Concern." *Forbes.* October 20, 2012. http://www.forbes.com/sites/rickungar/2012/10/20/romney-family-investment-ties-to-voting-machine-company-that-could-decide-the-election-causes-concern/ (accessed October 30, 2012).

United States Department of Commerce. *Censtats Databases.* 2013. http://censtats.census.gov/ (accessed February 12, 2013).

Verified Voting Foundation. "Letter to the President." *VerifiedVoting.org.* December 5, 2012. https://www.verifiedvoting.org/docs/presidentletter/ (accessed March 2, 2013).

—. *The Verifier.* 2012. http://www.verifiedvoting.org/verifier/ (accessed September 23, 2012).

Virginia State Board of Electors. "November 2008 Official Results." *Virginia State Board of Electors.* 2009. https://www.voterinfo.sbe.virginia.gov/election/DATA/2008/07261AFC-9ED3-410F-B07D-84D014AB2C6B/Official/96_s.shtml (accessed February 12, 2013).

"Voter Intimidation." New Orleans LA: New Orleans "Mascot", 1892.

"Votomatic Vote Recorder." *Smithsonian Institute.* 2004. http://americanhistory.si.edu/vote/resources_votomatic.html (accessed November 22, 2012).

Wagner, David. *Responses To Questions For The Record.* Berkeley, CA: University of California Berkeley, 2006.

Wagner, David. *Voting Systems Audit Log Study.* Berkeley, CA: Office of the California Secretary of State, 2010.

Wagner, Mackenzie, and Elizabeth Titus. "7 controversial voter ID quotes." July 11, 2012. http://www.politico.com/gallery/2012/07/7-controversial-voter-id-quotes/000265-003381.html (accessed January 24, 2013).

Wall Street Journal Editors. "Minnesota's Missing Votes: Some Senate absentee ballots are more equal than others." *Wall Street Journal.* April 18, 2009. http://online.wsj.com/article/SB124000875842430603.html (accessed January 15, 2013).

Wallach, Dan S. *Security and Reliability of Webb County's ES&S Voting System and the March '06 Primary Election.* Houston, TX: Rice University, 2006.

WarDriving.com. *War Driving.* 2012. http://www.wardriving.com/ (accessed February 3, 2013).

Weldemariam, Komminist, Richard A. Kemmerer, and Adolfo Villafiorita. "Formal Specification and Alalysis of an e-Voting System." Krakow, Poland: International Conference on Availability, Reliability and Security, 2010.

Whitmer, Clair. "What the Move Act Means For You." *Overseas Voter Foundation.* January 16, 2012. https://www.overseasvotefoundation.org/node/282 (accessed December 12, 2012).

Williams, Joel. "Massachusetts rep resigns amid voter fraud charges." *BallotNews.org.* December 23, 2012. http://ballotnews.org/2012/12/26/massachusetts-rep-resigns-amid-voter-fraud-charges/ (accessed December 26, 2012).

Wolchok, Scott, Eric Wustrow, Dawn Isabel, and J. Alex Halderman. "Attacking the Washington D.C. Internet Voting System." Bonaire: Conference on Financial Cryptography & Data Security, 2012.

Yasinsac, Alec, et al. *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware.* Tallahassee, FL: Security and Assurance in Information Technology Laboratory Florida State University, 2007.

Yee, Ka-Ping, David Wagner, Marti Hearst, and Steven M. Bellovin. "Prerendered User Interfaces for Higher-Assurance Electronic Voting." Vancouver, Canada: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop, 2006.

Zetter, Kim. "Aussies Do It Right: E-Voting." *Wired Magazine.* November 3, 2003. http://www.wired.com/techbiz/media/news/2003/11/61045?currentPage=all (accessed Decemebr 3, 2012).

—. "Building Better Voting Machines." October 18, 2006. http://www.wired.com/politics/security/news/2006/10/71957?currentPage=all (accessed November 10, 2012).

—. "Diebold Unloads Beleaguered Voting Machine Division." *Wired Magazine.* September 3, 2009. http://www.wired.com/threatlevel/2009/09/diebold-sells/ (accessed February 3, 2013).