VOTING SYSTEM RISK ASSESSMENT VIA COMPUTATIONAL COMPLEXITY ANALYSIS

Dan S. Wallach*

ABSTRACT

Any voting system must be designed to resist a variety of failures, ranging from inadvertent misconfiguration to intentional tampering. The problem with conducting analyses of these issues, particularly across widely divergent technologies, is that it is very difficult to make apples-to-apples comparisons. This paper considers the use of a standard technique used in the analysis of algorithms, namely complexity analysis with its "big-O" notation, which can provide a high-level abstraction that allows for direct comparisons across voting systems. We avoid the need for making unreliable estimates of the probability a system might be hacked or of the cost of bribing key players in the election process to assist in an attack. Instead, we will consider attacks from the perspective of how they scale with the size of an election. We distinguish attacks by whether they require effort proportional to the number of voters, effort proportional to the number of poll workers, or a constant amount of effort in order to influence every vote in a county. Attacks requiring proportionately less effort are correspondingly more powerful and thus require more attention to countermeasures and mitigation strategies. We perform this analysis on a variety of voting systems in their full procedural context, including optical scanned paper ballots, electronic voting systems, both with and without paper trails, Internet-based voting schemes, and future cryptographic techniques.

INTRODUCTION

The United States Elections Assistance Commission (EAC) recently solicited submissions for how it might assess the risks of voting systems.[1] According to its solicitation:

---

* Department of Computer Science, Rice University. The author wishes to thank Aaron Burstein, Ed Felten, Joe Hall, David Jefferson, Doug Jones, Eric Rescorla, David Wagner, and Nick Weaver for their comments on drafts of this Article. This work was supported in part by NSF grants CNS-0524211 and CNS-0509297.

[1] *See* United States Election Assistance Commission, Request for Information—Voting Systems Risk Assessment, http://www.eac.gov/voting%20systems/voluntary-voting-guidelines/request-for-information-2013-voting-systems-risk-assessment-support (last visited Oct. 6, 2008) [hereinafter Request for Information].

> The first phase will create reference models to be used in the assessment. This includes developing election process models to describe the operational context in which voting systems are used. It also entails developing voting systems models by generic technology type. This is needed because the types of threats encountered and their potential impacts vary by technology.[2]

The EAC asked the public to suggest how it might develop these models, with submissions due in April 2008.[3] While these submissions have not yet been made available to the public, we will discuss some prior work on this topic and then propose our own solution to this problem.

Clearly, we need an objective, quantifiable method for comparing voting systems.[4] Election officials who might purchase one system over another need to be able to concisely understand the relative insecurities of one product versus another.[5] Security analysts, testing authorities, and regulators need common ground for both setting a lower bound on acceptable security and for explaining how much better a system is than whatever the minimum standard requires.[6]

Qualitative analyses are, for better or worse, the standard method used to make arguments.[7] To pick a well-known example, the U.S. military was investigating the possibility of allowing its soldiers to vote, from overseas locations, via the Internet. They convened a panel of experts to conduct a security review. Several of the experts wrote a "minority report" expressing their concerns with the project,[8] leading to its cancellation and replacement with a fax-based system.[9] Alvarez and Hall criticize this

---

[2] United States Election Assistance Commission, Risk Assessment Summary, http://www.eac.gov/voting%20systems/voluntary-voting-guidelines/docs/risk-assessment-summary/ (last visited Oct. 6, 2008).

[3] *See* Request for Information, *supra* note 1.

[4] *See* Aaron Burstein et al., Comment on the U.S. Election Assistance Commission's Request for Information Regarding Voting Systems Risk Assessment Support 1 (2008), http://josephhall.org/papers/ucb-eacrficomment-20080428.pdf.

[5] *See* ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING 29–33 (Richard Celeste et al. eds., 2006).

[6] R. MICHAEL ALVAREZ & THAD E. HALL, ELECTRONIC ELECTIONS: THE PERILS AND PREMISES OF DIGITAL DEMOCRACY 45 (2008).

[7] *See* ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING, *supra* note 5, at 59–62, 68–69; BRENNAN CTR. FOR JUSTICE, THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD 9 (2006) [hereinafter MACHINERY OF DEMOCRACY], *available at* http://www.brennancenter.org/dynamic/subpages/download_file_39288.pdf.

[8] *See, e.g.*, DAVID JEFFERSON ET AL., A SECURITY ANALYSIS OF THE SECURE ELECTRONIC REGISTRATION AND VOTING EXPERIMENT (SERVE) 2–3 (2004), http://www.servesecurityreport.org/paper.pdf. The minority report will be referred to as the SERVE (secure electronic registration and voting experiment) report.

[9] *See* ALVAREZ & HALL, *supra* note 6, at 85.

outcome stating, "In the end, a small but vocal segment of the scientific community opposed the use of scientific experimentation in voting systems and technologies."[10] While the SERVE report's authors were concerned about the fundamental unsuitability of standard consumer platforms (e.g., Microsoft Windows XP plus Internet Explorer), with the risks of viruses, worms, or other forms of malware that could easily be engineered to compromise an election,[11] Alvarez and Hall felt that

> the central argument in this critique was overly general, ignored the reality of UOCAVA voting,[12] and ignored what would have been a broad array of project, procedural, and architectural details of the SERVE registration and voting system, which in all likelihood would have minimized or mitigated their concerns had the system been used in the planned trial.[13]

The SERVE report's authors are absolutely correct in that the weaknesses of Internet voting are the fundamental properties of how the Internet clients and servers operate. However, Alvarez and Hall have a valid point when they later note that other overseas votes are cast by fax, with its own attendant risks.[14] With disputes like these, we need a useful way of getting to some kind of ground truth.

I. OVERVIEW OF RISK ASSESSMENT FRAMEWORKS

A. Security Metrics

There are many different ways to quantify how secure or insecure a voting system (or any system) might be, but most of them require us to make approximations and guesses, among other problems.[15] Burstein et al., in their submission to the EAC request, make the point that there may well be no one-size-fits-all solution to this problem.[16] Nonetheless, we can consider a variety of possibilities.

---

[10] *Id.* at 77.

[11] *See* JEFFERSON ET AL., *supra* note 8, at 12–15.

[12] The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) was enacted by Congress in 1986. *See* 42 U.S.C. §§ 1973ff to ff-6 (2000). UOCAVA requires that the states and territories allow certain groups of citizens to register and vote absentee in elections for federal offices. In addition, most states and territories have their own laws allowing citizens covered by UOCAVA to register and vote absentee in state and local elections as well. *See* U.S. DEP'T OF JUSTICE, CIVIL RIGHTS DIV., THE UNIFORMED AND OVERSEAS CITIZENS ABSENTEE VOTING ACT, http://www.usdoj.gov/crt/voting/misc/activ_uoc.htm (last visited Oct. 6, 2008).

[13] ALVAREZ & HALL, *supra* note 6, at 85.

[14] *See id.* at 87.

[15] *See* Burstein et al., *supra* note 4, at 3–4.

[16] *Id.* at 5.

Threat taxonomies. Jones discusses the possibility of cataloging known threats against voting systems and creating a taxonomy of those threats.[17] The main benefit of this activity is that it helps security analysts identify areas where additional analysis might be desirable.[18] The presence or absence of any particular flaw does not, in and of itself, make it any easier or harder to attack a voting system. An attacker only needs to find one serious flaw in order to cause significant damage.

Voter performance metrics. Voters are regularly surveyed both before and after elections as to whom they support for a political office. Voters are also surveyed, perhaps more rarely, about how well they enjoyed the voting experience, how easily they could find their local precinct, and so forth. Ultimately, any survey or scientific study of voters can measure three useful properties of a voting experience: accuracy, efficiency, and satisfaction.[19]

Accuracy refers to how well a voting system captures the voter's intent.[20] While "residual votes" (e.g., spoiled ballots) offer a proxy measurement for accuracy, these measurements can also be taken in controlled laboratory conditions where experimental subjects have no anonymity (nor need for it), and thus their actual votes can be examined directly. Efficiency is simply the amount of time it takes to complete the voting procedure. Accuracy and efficiency can be objectively measured, while satisfaction relies on the voter's subjective opinions, stated in response to standardized questions. All of these dimensions of voter performance are quantifiable, and provide valuable metrics for examining how well a voting system performs.

Unfortunately, none of these performance metrics have a strong relationship to security. Two electronic voting systems could appear absolutely identical, from the voter's perspective, while having completely different underpinnings with radically different security vulnerabilities. A malicious voting machine could change a vote without detection, but the voter might still love the experience. Voter performance metrics do matter in one critical fashion: voting system security procedures often depend on voters or poll workers following procedures correctly. For example, voters should verify the output of voter-verified paper audit trail (VVPAT) printers to ensure that it matches their intent. If voters cannot do this, then the security mechanism's effectiveness is blunted. We will discuss usability issues in more detail when we compare particular voting systems.

---

[17] Douglas W. Jones, Threats to Voting Systems (Oct. 2005) (manuscript submitted to NIST Workshop on Developing an Analysis of Threats to Voting Systems), http://www.cs.uiowa.edu/~jones/voting/nist2005.shtml.

[18] *See id.*

[19] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-766T, ELECTRONIC VOTING OFFERS OPPORTUNITIES AND PRESENTS CHALLENGES 24–25 (2004) [hereinafter GAO TESTIMONY], *available at* http://www.gao.gov/new.items/d04766t.pdf (statement of Randolph C. Hite, Director, GAO Information Technology Architecture and Systems, before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Governmental Reform).

[20] *Id.*

Probabilities of failure. We can measure many aspects of elections, but we cannot measure the odds that a security attack will occur. Election security in the past is not a good predictor of election security in the future. For example, new vulnerabilities may be discovered which change the security landscape overnight. Also, if insecure systems were used and successfully compromised, evidence that the compromise occurred will not necessarily be known or recognized. The lack of evidence for prior security attacks against electronic voting machines simply has no bearing on the degree to which they are vulnerable or might be compromised in the future.

Dollar or time-costs. A tempting metric is to attempt to quantify the dollar cost or man-hour cost of a security attack.[21] This becomes even more attractive if the cost can be expressed in terms of dollars per vote flipped or man-hours per vote flipped because it can then be compared against other forms of manipulating voters' behavior (e.g., television advertisements, direct mail, or phone calls).[22] We could even talk about the dollars or man-hours that must be invested "up front," perhaps as part of a reverse-engineering process conducted by an attacker, followed by a "per vote" cost afterward.[23] These metrics are somewhat satisfying, in that they can be easily compared across different voting technologies, but there will be huge errors in any estimates.[24] Will it take one month or three months to reverse-engineer a voting machine and find an exploitable security bug?

Imagine that the bug in question allows an attacker to violate voters' anonymity but not flip their votes. What, then, is the cost per voter for bribing them to vote in a particular fashion? A related metric, raised by the Brennan Center Security Report, is the number of people who must be involved in a conspiracy to compromise a voting system.[25] If more conspirators are required, it would be that much harder for the attack to go off without detection.[26] As with dollar or man-hour costs, it is difficult to estimate these numbers accurately, except when only a single person is necessary to accomplish an attack.[27] In many scenarios, this is unrealistic.[28]

Complexity analysis. After rejecting all of these metrics, we need an alternative. For this, we turn to a technique used widely in the analysis of algorithms: complexity analysis.[29] Consider being given a pile of insurance forms, each coded with the client's customer ID number. We are assigned to take this unsorted pile and sort it such that the customer IDs are strictly increasing through the pile.[30] We might start

---

[21] *See* MACHINERY OF DEMOCRACY, *supra* note 7, at 115.

[22] *See id.*

[23] *See id.*

[24] *See id.* at 9–10, 115.

[25] *See id.* at 9.

[26] *Id.*

[27] *Id.* at 12–13.

[28] *Id.*

[29] THOMAS H. CORMEN ET AL., INTRODUCTION TO ALGORITHMS 44–45 (2d ed. 2001).

[30] A mind-numbing summer job performed by the author while he was in junior high school.

a new pile, on the side, in sorted order. Then, for each page from the unsorted pile, we flip through the sorted pile to find where it belongs. This first technique, called an *insertion sort*, will take time proportional to the number of pages (N), squared, as we have to insert N pages, and each might require us to flip through the whole stack, which can have up to N pages in it.[31] We might instead start by sorting by the *last* digit in the ID (the one's digit) into ten separate buckets, putting everything back together again, then sorting again by the second digit (the ten's digit), and so forth. This second technique, called a *radix sort*, takes time proportional to the product of the number of pages and the number of digits.[32] Another technique, cleverly called a *quick sort*, has us randomly pick a "pivot," separating the pages into two piles (those less than and those greater than the pivot).[33] Then for each smaller pile, we pick another pivot and repeat. That process turns out to take an expected time proportional to the number of pages multiplied by the logarithm of the number of pages.[34]

The benefit of this style of analysis, called complexity analysis, is that we can take very different procedures for sorting a pile of paper and focus on a very high level consideration of the effort we might expend.[35] We do not have to worry about whether it is slightly faster to shuffle the pages in a radix sort or in a quick sort, or to even worry about the variations that might occur from one run of the procedure to the next. Instead, this technique requires a rough estimate of the number of operations that we need to perform in proportion to the size of the problem.

This style of analysis is typically expressed with "big-O" notation.[36] Formally,

> $O(g(n))$ = a function $f(n)$, such that there exists positive constants c and n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$.[37]

In other words, if an algorithm is $O(N^2)$ (pronounced "order N-squared"), we are saying that the cost of the algorithm approaches some constant times N^2. If, however, N is small, then there are no guarantees, but it does not really matter, for these purposes, because the running time of the algorithm will not be big enough to matter.[38] In this framework, insertion sort is $O(N^2)$, radix sort with k digit-numbers is $O(kN)$, and quick sort is $O(N \log N)$. Among other clever properties, you can add these O-expressions together, and the more expensive operation will dominate the cheaper one. For example, if you have to first pick up the pile of pages from a mess on the floor, an $O(N)$ process, then quick-sort them, taking $O(N \log N)$ time, the

---

[31] CORMEN ET AL., *supra* note 29, at 23–25.
[32] *Id.* at 170–73.
[33] *Id.* at 145–58.
[34] *See id.* at 156.
[35] *See id.* at 41.
[36] *See id.* at 44.
[37] *See id.*
[38] *See id.* at 42.

sorting time will dominate the pick-up time, so the total cost O(N) + O(N log N) is equivalent to O(N log N). This sort of complexity analysis is fundamental to the theory of computer science, and detailed treatments of it can be found in most any CS theory textbook.

Similarly, big-O notation is a convenient way to evaluate election security. We can refer to attack costs in terms of the number of precincts or poll workers[39] (P), or the number of voters (N), among other possibilities.[40] This style of analysis tends to discount the upfront cost of discovering a bug (it is a constant, even if it is a big constant) while focusing on the scalability of the attack.[41] Big-O analyses provide a more precise characterization for what are commonly referred to as "retail" versus "wholesale" attacks. If an attack requires you to bribe each voter individually, we would say it is an O(N) attack, regardless of the number of attackers required to accomplish the attack.

Our model must indicate how we deal with scalability. If we have P poll workers attacking N ballots, then each poll worker might well perform O(N/P) work. Ultimately, the interest is in the incremental cost of corrupting N ballots. If each poll worker already handles N/P ballots, and the incremental cost of their corrupt behavior is negligible, then we would prefer to say that there is a total O(P) cost in corrupting N ballots. For example, you may need to get all P poll workers involved if you want to tamper with N ballots while they are still in the precinct. In this case, the dominating cost of the election fraud is getting the poll workers on board, while the incremental work per poll worker is negligible. In this way, our complexity analysis can subsume the Brennan Center Security Report's notion of counting the people required, when that is the limiting factor.

The strongest possible attacks would then be O(1), "constant" cost attacks. If one or a handful of attackers can change an arbitrary number of ballots, with minimal effort, that is as bad as an attack could possibly be. When we identify O(1) attacks on a voting system, that does not mean the voting system is necessarily unsuitable for use, but it means that extreme procedural measures must be taken to thwart such attacks. If such measures are infeasible, then the voting system really should not be used.

---

[39] Since there are a presumably constant number of poll workers per precinct, the O-expressions will be exactly the same in the analysis whether P refers to the number of poll workers or precincts. All that would change is the constant c, which disappears when we do this style of analysis.

[40] While one could argue that the number of poll workers is typically a constant fraction of the population (e.g., one poll worker for every hundred voters), and thus O(P) = O(N), the two order-of-magnitude difference between the sizes of these populations has a real impact on the viability of attacks conducted by poll workers versus attacks against individual voters. It is helpful if our analysis can distinguish corruption requiring P complicit poll workers versus N complicit voters.

[41] *See* CORMEN ET AL., *supra* note 29, at 41.

B. Attacker Goals

Before we conduct complexity analyses on specific voting systems, we first need to consider what an attacker's goals might be. The standard goals of any attacker in any security-relevant context are typically attacks against integrity, confidentiality, and availability.[42] Applying these to elections:

Integrity attacks aim to change the election totals.[43] A successful integrity attack is one that survives tallying, recounting, and any subsequent legal challenges. A simple integrity attack is stuffing ballots into a paper ballot box, combined with forged signatures in a poll book, to keep everything consistent. An integrity attack, in this definition, must go undetected, lest the results be overturned or the election redone from scratch.

Confidentiality or anonymity attacks are a different game.[44] If we can violate the anonymity of voters through whatever means, then we can potentially bribe or coerce them to vote however we want. In this case, the election tallies may be entirely accurate with respect to capturing the voters' *stated* intent, but the election results may nonetheless not represent the true preferences of the voters.[45]

Availability attacks (also called denial-of-service attacks or DoS) are attempts to disrupt the election and can be as simple as physically destroying a voting system, stealing a ballot box, or cutting power to a building.[46] DoS attacks, selectively applied, may introduce biases that affect the election outcome, but they make no attempt at stealth (e.g., destroying ballot boxes from precincts with known biases).[47] A DoS attack may have as its goal to simply cause a chaotic outcome, or no outcome at all.[48] Or, a DoS attack may be acceptable to the attacker if the whole world knows the results are corrupt, but regular election procedures will have no way to correct the errors and might then accept the faulty results. In this respect, an integrity attack that is discovered but cannot be undone would, by our definition, be a DoS attack.[49] (Perhaps such attacks could also be classified as "integrity" attacks, but the victor in such a race would lack some of the legitimacy that can come from a "clean" victory.)

When considering these classes of election attacks against various election systems, we must make a number of simplifying assumptions. First, we will assume that an attack is focused on a specific county, voting uniformly on a single technology. An attack against one county would not have an impact on surrounding counties.[50]

---

[42] *See* GAO TESTIMONY, *supra* note 19, at 24–25.

[43] *See id.* at 25.

[44] JEFFERSON ET AL., *supra* note 8, at 16–17.

[45] *Id.*

[46] *See id.* at 18–19.

[47] *See id.* at 19.

[48] *See id.* at 18–19.

[49] *See id.* at 18–20.

[50] In Georgia and Maryland, the whole state votes monolithically on the same electronic voting system, with centralized resources to maintain their machines. *See* Campaign for

Instead, each county would need to be separately attacked. Clearly, the cost of attacking a county with two separate systems is equal to the sum of the costs for attacking the individual systems. We will also assume that prospective attackers already know the design and implementation of particular voting technologies. Security must come either from the strengths of those designs or from the strengths of poll workers and election officials following procedures correctly.

For every attack we consider, we will consider three variants: attacks originating from "normal" voters; attacks originating from poll workers, postal employees, and other intermediaries; and attacks originating from insiders at the election headquarters. Corrupt insiders obviously pose a greater threat than corrupt voters, requiring correspondingly stronger mechanisms to mitigate against the possibility of such corruption.

For this analysis, we do not consider pattern voting attacks (also sometimes called the "Italian attack"), where a voter uses unimportant races to encode a unique ID number, then votes as he or she has been bribed to do on the important races. To the extent that this attack is a problem, it is a problem on absolutely any voting system that can produce complete ballot records. In schemes where nobody ever sees the raw ballots (including VoteBox,[51] discussed in more detail below), this would never be a viable attack.

C. Example Cases

Under this set of attacker goals, there are some ambiguous cases that are worth considering. In Zimbabwe's recent presidential election, Robert Mugabe initially lost his re-election bid to Morgan Tsvangirai,[52] and then won a revote where his opponent withdrew amid widespread state-sponsored violence.[53] In this case, voters were still asked to vote, but there is no question that the will of the people was not reflected in the outcome. The violence was inflicted upon large swathes of the Zimbabwe population, so we would consider it an O(N) attack. Certainly, there was no stealth or

---

Verifiable Voting in Maryland, An Open Letter to House and Senate Ways and Means Committee, http://www.truevotemd.org/take_action.asp (last visited Oct. 6, 2008); Press Release, Karen Handel, Ga. Sec'y of State, Secretary Cox Announces Selection of Diebold Election Systems to Provide New Statewide Electronic Voting System (May 3, 2002), *available at* http://sos.georgia.gov/pressrel/050302.htm (discussing a contract that the state of Georgia has with Kennesaw State University to do many aspects of its election administration). In a scenario like this, a simplification is to treat the state as if it were a single, large county. For constant-cost attacks, this is likely to be an accurate model.

[51] *See generally* Daniel Sandler et al., *VoteBox: A Tamper-Evident, Verifiable Electronic Voting System*, 17 USENIX SECURITY SYMP. 349 (2008), *available at* http://www.usenix.org/events/sec08/tech/full_papers/sandler/sandler.pdf.

[52] *See* Barry Bearak, *Mugabe Foes Win Majority in Zimbabwe*, N.Y. TIMES, Apr. 3, 2008, at A1.

[53] *See* Celia W. Dugger & Barry Bearak, *Mugabe Is Sworn in to Sixth Term After Victory in One-Candidate Runoff*, N.Y. TIMES, June 30, 2008, at A8.

subterfuge as part of the attacks. Instead, the forced withdrawal of Tsvangirai is best described as a DoS attack. Now, Tsvangirai and his immediate deputies were also personally subject to harassment and violence, and were forbidden access to state-controlled news media.[54] This could be classified as an O(1) DoS attack. There were also allegations of voters' anonymity being systematically violated at the polls: an O(*N*) confidentiality attack. Unsurprisingly, the legitimacy of Mugabe's victory is easy to call into question.

A similar instructive example is the election of "landslide" Lyndon Johnson for the U.S. Senate in 1948.[55] Texas, at the time, was largely controlled by the Democratic Party, so the Democratic primary election was to be decisive for who would win the Senate seat.[56] In that election, which went to a runoff between Johnson and former Texas Governor Coke Stevenson, Johnson defeated Stevenson by an "87-vote landslide."[57] Much attention has focused on ballot stuffing in Jim Wells County's infamous "Box 13," but ballot box stuffing, among other fraudulent behavior, was apparently the norm across the state.[58] Counties were allowed to report "revisions" to their tallies in the week following the election, allowing local party bosses to continuously adjust their vote totals to assist their preferred candidate.[59] Baum and Hailey note that, had the original, unrevised tallies been used, Johnson would have still defeated Stevenson by 506 votes.[60] They conclude that Johnson won largely on the strength of his turnout efforts, or rather the lackluster turnout efforts of his opponent.[61]

Classifying the attacks in this race is tricky. Individual voters' poll taxes were often paid by the political campaigns, but their votes were still ostensibly cast privately.[62] Still, a well-funded operation to pay for more voters would be classifiable as an O(*N*) integrity attack, since each voter was individually brought in. This assumes a candidate's operation can accurately select its supporters, to pay their poll taxes, without paying for its competition. Ballot stuffing and poll book manipulation is clearly O(*P*), since there are *P* ballot boxes that would need to be compromised, but is it an integrity attack or a DoS attack? The "Box 13" story is all about the discovery of clearly fraudulent signatures in the poll books, and similar fraud likely occurred elsewhere in the state without undergoing the same level of scrutiny.[63] Based on our scheme, the clear presence of the "Box 13" fraud, combined with the inability of

---

[54] *Id.*

[55] *See* Dale Baum & James L. Hailey, *Lyndon Johnson's Victory in the 1948 Texas Senate Race: A Reappraisal*, 109 POL. SCI. Q. 595 (1994).

[56] *See id.* at 596.

[57] *See id.* at 595.

[58] *See id.* at 596.

[59] *See id.* at 610.

[60] *Id.*

[61] *See id.* at 598–99.

[62] *See id.* at 604.

[63] *See id.* at 608–10.

anybody to correct the problem, would make it a DoS attack, while other ballot-stuffing events that went undiscovered would be integrity attacks. In other words, ballot stuffing can be a successful attack, whether or not it is discovered, so long as the election results are not thrown out and the election redone from scratch.[64]

II. APPLYING COMPLEXITY ANALYSIS TO VOTING SYSTEMS

A. Absentee Paper Voting (Vote-by-Mail)

All of Oregon's voters cast their votes by mail, with a large number of voters in other states increasingly preferring this voting mechanism for its comfort and convenience.[65] Of course, by voting in an unsupervised location (i.e., in the voter's home), there is no enforcement of anonymity for voters. This means that vote selling, by voters, is an O(*N*) attack, because each voter must individually be bribed or coerced. The postal mail is likewise far from a safe and secure delivery channel. With *P* postal workers (simplifying assumption: the number of postal mail routes is proportionate to the number of voting precincts), one could imagine a variety of O(*P*) confidentiality attacks (example: steaming open envelopes to read their contents, with each of the *P* postal workers reading *N*/*P* ballots). Once postal votes reach the election headquarters, confidentiality attacks potentially drop to as low as an O(1) cost, requiring at most a handful of corrupt election workers.

Integrity attacks and DoS attacks will follow the same pattern. Individual voters could individually modify ballots from their neighbor, spouse, tenants, and so forth—O(*N*) effort—requiring nothing more sophisticated than steam to open an envelope, or fire to destroy one. Similarly, *P* postal workers could open envelopes and either spoil undesirable ballots, substitute alternative ballots, or simply fail to deliver those ballots—an O(*P*) attack. Election headquarters employees can potentially mount O(1) integrity and DoS attacks, since they are already individually handling each ballot. The postal system has large central sorting facilities. Employees in these locations could potentially mount O(1) DoS attacks (e.g., destroying ballots from particular zip codes), but their ability to mount integrity attacks would vary. In a large city, the speed with which mail is processed would preclude centrally attacking individual envelopes.[66] In smaller towns and counties, O(1) postal attacks against integrity might also be possible.

---

[64] *See* Sarah P. Everett, *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection* 28 (May 2007) (unpublished Ph.D. thesis, Rice University) (on file with author).

[65] *See* H.R. REP. NO. 110-581, at 3 (2008).

[66] *Cf.* Press Release, U.S. Postal Serv., Postal Service High-Speed Sorters Get Smarter, Faster: Board of Governors Approve Funding for New Technology (Apr. 2, 2008), *available at* http://www.usps.com/communications/newsroom/2008/pr08_032.htm.

The existence of these O(1) attacks clearly demands strong procedural controls to prevent them, such as "separation of privilege" procedures where, for example, one worker examines the outer envelope for voter registration information, passing along an inner envelope, holding the ballot, to a separate worker who does not know the identity of the original voter. Of course, both workers could collude and defeat the system. Additional measures, such as having many more employees dividing the labor, installing round-the-clock video surveillance of areas where ballots are handled, or having ballots with hidden marks passing through the system as a check against tampering would certainly be appropriate.[67] Even if the resulting system is still vulnerable to O(1) attacks, additional constant factors of difficulty are far better than nothing. Similarly, the risks from the postal channel would seem to require sophisticated tamper-evident envelopes.[68] If the effort necessary to steam open an envelope without detection was sufficiently high, it might become infeasible for regular postal workers to open and modify ballots without taking too much time, and thus being more easily detected.[69]

B. Paperless, Electronic Voting Systems

Direct recording electronic (DRE) voting system vendors have made a number of claims about their security. Following the California "Top to Bottom" Reports, the Ohio EVEREST Reports, and the Florida "SAIT" study conducted in the wake of the Sarasota 2006 problem, we now know many of these claims to be false.[70] Based on that work, for every major commercial DRE voting system used in the U.S., we can summarize these systems' security as follows.

Anonymity attacks require O(*P*) effort. *P* poll workers would need to each record the order in which voters appeared before each machine—a minimal additional effort beyond the work they already perform as part of the voter registration process. In some states, voter sign-in logs are already recorded in order, as a matter

---

[67] *See* SRINIVAS INGUVA ET AL., SOURCE CODE REVIEW OF THE HART INTERCIVIC VOTING SYSTEM 18 (July 20, 2007), http://www.sos.ca.gov/elections/voting_systems/ttbr/Hart-source-public.pdf (report commissioned as part of the California Secretary of State's "Top-to-Bottom" Review of California Voting Systems).

[68] *See generally* Tal Moran & Moni Naor, *Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol*, 25 ADVANCES IN CRYPTOLOGY 88 (2006) (suggesting methods of increasing envelope security).

[69] *See id.*

[70] *See generally* JOSEPH A. CALANDRINO ET AL., SOURCE CODE REVIEW OF THE DIEBOLD VOTING SYSTEM (July 20, 2007) (on file with author); OHIO SEC'Y OF STATE, EVEREST PROJECT, PROJECT EXECUTIVE SUMMARY REPORT (2008) [hereinafter EVEREST REPORT], *available at* http://www.sos.state.oh.us/SOS/upload/everest/00-SecretarysEVERESTExecutiveReport.pdf; ALEC YASINSAC ET AL., SOFTWARE REVIEW AND SECURITY ANALYSIS FOR THE ES&S IVOTRONIC 8.0.1.2 VOTING MACHINE FIRMWARE (2007) [hereinafter SAIT STUDY], *available at* http://www.cs.berkeley.edu/~daw/papers/sarasota07.pdf.

of course, dropping the complexity of the attack to O(1), since no poll workers must be corrupted! After that, due to poor engineering of the DRE systems, including easy poll worker access to the ballot records, the order in which votes were cast can be recovered from the electronic records kept by these systems.[71] A variety of engineering tactics can and should be taken to improve this situation, but none are yet deployed.[72] In the best possible case, however, we could still imagine O(*P*) attacks that do not rely on poor engineering of the voting machines. As an example, small video cameras could be surreptitiously installed in the ceiling above a machine to record its screen as it is used. Consequently, improving anonymity attacks beyond O(*P*) will be a difficult problem to tackle.

Due to poor engineering practices of the DRE vendors, integrity and DoS attacks require O(1) effort for normal voters—the worst possible case. The California, Ohio, and Florida analyses discovered "viral" attacks against these voting systems.[73] A single attacker, tampering with a single voting system, can inject a custom-engineered virus.[74] This virus can then take advantage of the poor software engineering of other parts of the voting system and spread from one voting machine to another, based entirely on the usual procedures carried out by election officials.[75] In the case of Diebold's DRE systems, the virus can spread through the smartcards used to authorize the machines to accept votes.[76] In the case of Hart InterCivic's DRE system, one DRE can infect a back-end system used in the election administration's warehouse for inventory control, among other purposes.[77] This system can then infect any subsequent DRE connected to it.[78] An infection introduced in one election can then be present in *every* voting machine used by the county in its subsequent elections.[79] This infection could then have a variety of negative behaviors, ranging from flipping

---

[71] *See* J. Alex Halderman et al., *You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems*, 2008 USENIX/ACCURATE ELECTRONIC VOTING TECH. WORKSHOP, § 5.2, *available at* http://www.usenix.org/events/evt08/tech/full_papers/halderman/halderman.pdf.

[72] *See id.* at Abstract.

[73] *See id.* at § 1.3; *see also* CALANDRINO ET AL., *supra* note 70; EVEREST REPORT, *supra* note 70; SAIT STUDY, *supra* note 70.

[74] *See* Halderman et al., at § 1. A side question is whether a normal voter might have sufficient access to open the case of a voting machine or otherwise conduct an attack. In practice, voting machines are often left unguarded in relatively public places. Furthermore, some vendors support a "curb-side voting" procedure, where disabled voters who cannot physically enter the polling place can be accommodated by bringing voting machines out to them instead. Curb-side voting gives attackers the necessary time and privacy to conduct an attack. Many of the attacks could even be conducted by a voter while in the voting booth.

[75] *See id.*

[76] *See* Everett, *supra* note 64, at 28–29.

[77] *See* INGUVA ET AL., *supra* note 67, at 77.

[78] *See id.*

[79] *See id.*

votes through simply deleting them en masse.[80] If the vendors were to repair all the bugs found in these studies, and no other bugs remained to be discovered, these attacks would become O(*P*)—poll workers would need to tamper with each physical voting system to cause it to misbehave.

A number of procedural measures are commonly suggested for dealing with some of these vulnerabilities. "Logic and accuracy testing" (L&A testing) typically involves casting a handful of votes for each candidate and then tabulating the votes.[81] It is trivial for a tampered machine to determine when it is being tested like this and to behave correctly.[82] Likewise, L&A testing, conducted by election officials prior to an election, cannot detect tampering conducted by poll workers or normal voters once machines are in the field.[83] L&A testing, if not conducted carefully, can even result in test votes that appear in the final election tally.[84] Similarly, "hash code testing," a process for verifying that the software inside a voting machine matches the software that is *supposed* to be there, is ineffectual against sophisticated attackers, who can arrange for a corrupt machine to respond as a proper machine would to any of the tests.[85] As an example, Hart InterCivic's system has a very detailed mechanism intended to detect code tampering.[86] But, the California review found it to be easily subverted.[87]

Parallel testing takes a set of voting machines, randomly pulled from general circulation, and instead tests them, on election day, in a controlled and videotaped environment.[88] Any misbehavior of the voting machines would then be caught. Parallel testing procedures can discover the presence of many (but not necessarily all) integrity and DoS attacks, but will have no effect on anonymity attacks, or attacks that are installed by poll workers or attackers, on the site of specific precincts when the election begins.[89] Likewise, while parallel testing might discover such attacks, it offers no way to prevent them or recover from them.[90] At its best, parallel testing converts integrity attacks, previously undetected, into DoS attacks, without itself offering any way to recover the original intent of the voters.[91]

---

[80] *See* Everett, *supra* note 64, at 30.

[81] *See* INGUVA ET AL., *supra* note 67, at 79–82.

[82] *See id.*

[83] *See id.* at 82.

[84] *See* DAN S. WALLACH, SECURITY AND RELIABILITY OF WEBB COUNTY'S ES&S VOTING SYSTEM AND THE MARCH '06 PRIMARY ELECTION (2006), *available at* http://accurate-voting.org/wp-content/uploads/2006/09/webb-report2.pdf (the author's expert report in *Flores v. Lopez*).

[85] *See* INGUVA ET AL., *supra* note 67, at 43.

[86] *See id.* at 42.

[87] *See id.* at 40.

[88] *See id.* at 81.

[89] *See id.* at 82.

[90] *See id.*

[91] *See id.*

C. Electronic Voting Machines with VVPAT Printers

In response to objections from computer scientists and activists, and to requirements by many states, DRE vendors now offer a variety of "voter-verified paper audit trail" (VVPAT) attachments for their machines.[92] The major U.S. vendors all use a reel-to-reel thermal printer, behind glass.[93] Voters may see the record of their vote but may not touch it. Because the paper is never cut, these devices record votes in the order cast.[94] For the purposes of this analysis, we will assume that these printers are actually working properly (versus anecdotal evidence that they suffer mechanical failures) and that voters will actually read them (even though controlled human subject experiments suggest that two-thirds would fail to see any discrepancies).[95]

Confidentiality attacks are still O(*P*), based purely on the electronic results being easily de-anonymized (as described above for paperless DRE systems, and would likewise drop to O(1) if poll workers or electronic poll books recorded the order in which voters appeared as their standard operating procedure). Additionally, the recording of votes in the order cast on the VVPAT paper tapes similarly allows for O(*P*) attacks.[96] If the paper were cut after each voter and piled up in a random order in a bag of some kind, then the VVPAT attachment would no longer be the most obvious way to conduct a confidentiality attack.[97]

Tampering and DoS attacks improve from O(1), with paperless DREs, to O(*P*), with VVPAT printers, by virtue of increasing the burden on the attacker. Now the attacker must also perform O(*P*) effort to consistently tamper with the VVPAT printouts. This implies that VVPAT, even poorly implemented, yields a significant complexity improvement relative to existing DREs' security performance. However, achieving this improvement requires that election officials reconcile the VVPAT results against the electronic results.[98] Given Everett's findings that many voters will fail to notice errors on VVPAT results,[99] election officials must be particularly attuned to even a very low rate of complaints, creating a secondary vulnerability, namely that voters could falsely claim to have observed discrepancies in order to cause perfectly good equipment to be removed from service—an O(*P*) DoS attack.[100]

In response to the California and Ohio studies, Halderman et al. considered mitigations that might improve the security of electronic voting systems. They describe

---

[92] *See, e.g.*, *id.* at 9 (discussing how VVPAT is required by law in California).

[93] *See id.* at 9, 15.

[94] *See id.* at 9.

[95] *See* Everett, *supra* note 64, at 1, 86.

[96] *See* INGUVA ET AL., *supra* note 67, at 9.

[97] *See, e.g.*, *id.* at 68 (discussing one method of maintaining recorded votes out of sequence, in an effort to increase voter anonymity).

[98] *See id.* at 75–76.

[99] Everett, *supra* note 64, at 86.

[100] *See* INGUVA ET AL., *supra* note 67, at 76.

detailed system-specific procedures that can mitigate many (but not all) O(1) attacks against these systems.[101] Their techniques expand on the concepts described above, and rely on having the VVPAT paper trails.[102] In the end, they cannot prevent integrity attacks, but they can limit the degree to which they spread and can increase the confidence with which they may be discovered.[103] On paperless DRE systems, variations on their techniques might improve some of the O(1) integrity attacks to O(*P*) attacks as well. Many of the mitigations proposed by Halderman et al. require custom hardware "gadgets" for purposes such as clearing memory cards.[104] No such gadgets exist, and it is unclear that such gadgets could legally be used without being certified by the appropriate federal and state authorities.[105]

D. Precinct-Based Optical Scan Systems

While some activists feel that the only safe way to vote is to count ballots by hand, optical scanning of ballots adds significant efficiencies to the process, particularly in modern American elections where voters may be asked to respond to thirty or forty separate issues. There are two main styles of ballot scanners: precinct-based scanners and central scanners. The former is attached to the top of a ballot box, while the latter is installed at the central election headquarters.[106] Precinct scanners can issue warnings or errors in cases of under- or over-voted ballots, potentially improving accuracy.[107] From a security perspective, the hand-marked paper ballots constitute a voter-verifiable paper trail, providing an independent path to determine the voters' intent, in cases where the electronic records may be called into question.[108] For this analysis, we will assume that the paper records are, indeed, reconciled against the electronic tallies. Without mandatory reconciliation or auditing, the security analysis would be much more pessimistic.

Precinct scanners offer comparable anonymity to any other technology.[109] A malicious scanner can record votes in the order in which they were cast—an O(*P*) attack, since *P* different scanners must be corrupted.[110] Vulnerabilities have been

---

[101] *See* Halderman, *supra* note 71.

[102] *See, e.g.*, *id.* (suggesting a 100% manual count of the VVPAT records).

[103] *Id.* at § 7.

[104] *Id.* at § 2.

[105] *See id.*

[106] *Id.* at § 1.4.

[107] MACHINERY OF DEMOCRACY, *supra* note 7, at 81; *see also* David Chaum et al., *Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems Using Invisible Ink Confirmation Codes*, 2008 USENIX/ACCURATE ELECTRONIC VOTING TECH. WORKSHOP, § 4.4 (2008), *available at* http://www.usenix.org/events/evt08/tech/full_papers/chaum/chaum.pdf.

[108] MACHINERY OF DEMOCRACY, *supra* note 7, at 82; Chaum et al., *supra* note 107, at § 1.

[109] Chaum et al., *supra* note 107, at § 5.2.

[110] *Cf. supra* Part I.A.

found in commercial optical scanners, as part of the California and Ohio studies, showing that even unmodified scanners are improperly engineered, allowing the order in which votes were cast to be recovered.[111] If these known-flawed optical scanners were used in precincts that recorded the order in which voters sign in, as a matter of regular procedure, that combination would lower the complexity of an anonymity attack to O(1).[112]

The integrity guarantees of precinct scanners are quite good, assuming proper auditing of the paper ballots occurs after the election. If the electronic records were compromised, the paper records could be used to reconstruct them, either via a different scanner or by hand. If the paper records were compromised, the electronic records could be used as a back-up. Successful integrity attacks are thus an O(*P*) process. An attacker would need to modify both the electronic records and the paper ballots in a consistent fashion and would need to attack each precinct in turn.

Precinct scanners resist DoS attacks reasonably well. Even in the worst case, if they are completely broken, poll workers can remove them from the ballot boxes, falling back on the central scanners. Still, precinct scanners are vulnerable to the variety of O(*P*) attacks that threaten any precinct (e.g., cutting the power), as well as attacks such as intercepting or spoiling the paper ballots while in transit.

Centrally scanned ballots, whether used as a fallback for failed precinct ballot scanners or just used for mail-in votes, are clearly subject to O(1) insider attacks. Auditing procedures would clearly be necessary to double-check that the electronic tallies correspond accurately to the paper ballots.

E. Internet Voting (Via Home Computers)

We can conduct all manner of high-dollar commerce on our home computers, so why not vote? Indeed, Estonia has done this, as have a handful of other elections.[113] Of course, there are significant differences between the world of e-commerce and the world of e-voting. Commercial fraud happens all the time (identity theft, etc.), leading to a huge industry that deals with this fraud. Nonetheless, e-commerce succeeds because the total volume of legitimate commerce dwarfs the volume and expense of fraud.

Furthermore, commercial transactions are not anonymous.[114] Customers, merchants, and their banks carefully record these transactions. If and when discrepancies arise, customers can challenge merchants, and everybody can settle on the proper

---

[111] *See, e.g.*, EVEREST REPORT , *supra* note 70, at 40–41.

[112] *Id.*

[113] Sutton Meagher, Comment, *When Personal Computers Are Transformed Into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights*, 23 AM. U. INT'L L. REV. 349, 355 (2008).

[114] *Id.* at 395–96.

outcome. In e-voting, however, votes must be anonymous. Without anonymity, bribery and coercion become valid O(N) threats against the election.

If we want to use home computers to vote over the Internet, that means dealing with Microsoft Windows and Internet Explorer, for which new security vulnerabilities are discovered on a depressingly regular basis (not to say that any other consumer computing platforms are necessarily any better in this regard). One of the key risks these vulnerabilities create is that attackers might focus their attacks specifically on people who are likely to vote using the Internet.[115] For example, if an attacker wanted to tamper with the Estonian online election, the attacker might first break into a popular Estonian web site (a new site, a bank site, etc.) and install some kind of malware that could then infect visitors to that site.[116] Likewise, many voters' computers can be directly attacked over their network connections.[117] Attackers can use a variety of "geo-location" techniques to focus their efforts exclusively on computers within the country being attacked.[118] Any machine that has been compromised would then presumably act normally except when visiting the election authority's web site.[119] At that point, it is trivial for the computer to show one thing to the voter while behaving in an arbitrarily different fashion on the network. Voters would have no way of knowing whether their votes had been flipped. In fact, a custom-engineered attack could erase itself subsequent to the election, leaving no trace of its presence.[120]

The Estonian government implemented a number of particular security measures, notably a requirement that voters use the national ID card, a "smartcard," in order to authenticate to the voting website.[121] Estonia also allows voters to cast multiple votes, with the last one counting. The government additionally allowed Internet voters to vote subsequently in person, canceling out any prior electronic vote.[122] With these mechanisms in mind, as they might well be copied with other Internet-based voting schemes,[123] we can analyze the security of many other proposed Internet voting systems.

Confidentiality attacks that rely on in-person observation of the voting process (i.e., somebody watching over your shoulder as you vote) are ostensibly defeated by

---

[115] *See* Aviel Rubin, *Security Considerations for Remote Electronic Voting Over the Internet*, http://www.avirubin.com/e-voting.security.pdf (last visited Nov. 14, 2008) (detailing Internet security considerations).

[116] *Cf. id.* at 3–4.

[117] *Id.*

[118] *Id.* For an example of software touting geo-location capabilities, visit http://www.ip2location.com.

[119] *Id.* at 9–10.

[120] *Id.*

[121] *See* Meagher, *supra* note 113, at 356–58.

[122] These facts are based upon personal observation of the author.

[123] *See* Meagher, *supra* note 113, at 351 n.4 (identifying other countries that have piloted Internet elections).

Estonia's multiple voting scheme, but in fact the attackers could well "borrow" the voters' ID cards. With these ID cards, attackers could prevent subsequent online votes and watch to make sure the voters do not attempt to go vote in person. These O(N) attacks would be very difficult to defeat. More worrisome is the fact that the back-end computers carefully track the binding between the voter and the more recently cast vote.[124] This procedure could allow malicious code, in the back-end, to observe these bindings—an O(1) attack. Likewise, malicious client-side code, installed in a viral fashion, could observe voters' actual behavior—another O(1) attack.

Integrity attacks on the client side would rely on breaking into the voters' home computers. It is difficult to estimate what percentage of these computers might be vulnerable to modern attack tools, but the cost of breaking in is O(1)—it is no more effort to break into one system than a thousand systems. There may also be O(1) integrity attacks against the server side, depending on the particular details of how the server has been implemented, how the cryptographic exchange works with the smart-card, and so forth.[125] Given the difficulty inherent in building a secure web-facing service, external attacks may always be feasible.[126] And, of course, insider attacks would also be O(1). If and when such attacks were detected, one could imagine heavyweight solutions, such as discarding online votes and requiring voters to appear in person. Clearly, an attacker would have to avoid the temptation to exert too much influence on the election outcome in order to fly below the radar.

DoS attacks are trivially available with O(1) effort. The elections web server has finite resources that can be easily exhausted by standard Internet attack tools that leverage vast numbers of compromised "zombie" computers to make requests as fast as possible of the server.[127] Such "distributed denial of service" (DDoS) attacks require extensive server-side resources to counter.[128] Google and Yahoo! engineers will privately admit that despite the massive scale of their operations, they still worry about DDoS attacks. If the biggest web services in the world have to worry about DDoS attacks, an elections web server is clearly in trouble. DDoS attacks can also be mounted against an entire country. Estonia, in fact, was attacked by (alleged) Russian hackers in 2007, crippling large parts of the country's Internet infrastructure.[129] To date, nobody has been charged with a crime.[130] If this were to occur during an

---

[124] *See id.* at 357.

[125] Rubin, *supra* note 115, at 6–8.

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN (Manchester, Eng.), May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

[130] Jose Nazario, *Estonian DDoS Attacks—A Summary to Date*, ARBOR NETWORKS SECURITY BLOG, May 17, 2007, http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

election, the Internet voting infrastructure would almost certainly fail. One could imagine a variety of draconian solutions, including disabling the Internet connection for the entire country. This measure would dampen attacks from outside the country, but would do nothing if attackers had compromised systems within the country, or set to mount their attacks autonomously.

In short, Internet voting in Estonia, via the failed SERVE project, or really any other way of using the Internet to connect personal computers' web browsers to web servers for purposes of casting votes, is subject to a variety of O(1) attacks. While Estonians can at least fall back to other voting technologies, the push to adopt Internet voting, even in limited trials, is inappropriately ignoring these glaring risks.

F. Future "End-to-End" Cryptographic Voting Systems

Cryptographers for the last two decades have been promoting a family of mathematical techniques that lead to a property called "end-to-end verification" of elections.[131] While specific techniques vary, there are several features these systems all have in common. Voters still cast votes in a polling place, requiring and ensuring their anonymity.[132] Whether using paper or an electronic voting machine, voters may optionally leave the polls with some kind of "receipt" that will allow them to identify a record corresponding to their vote on a public "bulletin board."[133] The bulletin board does not contain human-readable votes, but rather an encrypted form of the vote.[134] The tallying process requires the participation of one or more trusted parties, and ultimately yields both the election totals as well as a "proof" that can be verified by anybody.[135] Anybody can read the bulletin board and verify the computation that was used to derive the vote totals, even though they could not have performed the whole computation themselves.[136]

Other properties vary. One clever idea from Benaloh allows any voter to "challenge" any voting system to prove that it is properly encrypting the voter's ballot.[137] The idea is that a normal DRE system would go through its normal dialog with the voter until the voter agrees with the contents of the summary screen.[138] At

---

[131] *See* Chaum et al., *supra* note 107, at § 1 (defining end-to-end voting systems); *see also* Sandler et al., *supra* note 51, at 355 (defining end-to-end verifiable voting system as "one that can prove to the voter that (1) her vote was cast as intended and (2) her vote was counted as cast").

[132] Chaum et al., *supra* note 107, at § 3.

[133] *Id.*; Sandler et al., *supra* note 51, at 353.

[134] Sandler et al., *supra* note 51, at 352–53.

[135] *Id.*

[136] *Id.*; *see* Josh Benaloh, *Ballot Casting Assurance Via Voter-Initiated Poll Station Auditing*, 2 USENIX/ACCURATE ELECTRONIC VOTING TECH. WORKSHOP 1, 1–2 (2008) (highlighting the tension between vote encryption and voter-initiated auditing).

[137] *See* Benaloh, *supra* note 136, at 4–5.

[138] *Id.* at 5.

this point, the machine would generate the encrypted vote, sign it, and physically print it.[139] The voter sees the printing taking place.[140] At this point, the voter gets one new question: "would you like to cast this ballot or challenge it?" If the voter says "challenge," then the machine prints the encryption keys, allowing anybody to decrypt the vote and make sure that it is as the voter intended; this vote will *not* be counted.[141] If the voter says "cast," then the machine throws away the key and casts the vote.[142] These challenges allow roving election auditors to enter polling places while the election is ongoing, set up video cameras as in parallel testing, and verify that voting machines are behaving properly.[143] Unlike parallel testing, however, the machines being tested are the very live machines being used by real voters.[144] Variations on Benaloh's technique have already been implemented in two separate research voting systems (VoteBox[145] and Helios[146]).

In order to be concrete, we will analyze the security of VoteBox,[147] which feels to most voters like a DRE voting system, and Scantegrity II,[148] which feels to most voters like an optical scan voting system.

VoteBox, like any DRE, could be maliciously modified to record votes in the order cast.[149] Scantegrity, like any precinct optical scanner, has the same property. Both are thus subject to O(*P*) anonymity attacks.

VoteBox and Scantegrity have very strong mechanisms to detect integrity attacks. VoteBox's challenge mechanism can detect a misbehaving machine, as the election is ongoing.[150] Scantegrity looks and feels much like a regular paper ballot, so it inherits the integrity benefits of paper ballots.[151] Scantegrity also has mechanisms that

---

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] *Id.*; *see also* MACHINERY OF DEMOCRACY, *supra* note 7, at 18–19 (describing a regimen for parallel testing).

[144] Sandler et al., *supra* note 51, at 352 (describing the fundamental problem with parallel testing as being "artificial": "the conditions under which the test is performed are not identical to those of a real voter in a real election").

[145] *Id.* at 349.

[146] Ben Adida, *Helios: Web-Based Open-Audit Voting*, 17 USENIX SECURITY SYMP. 1 (2008), *available at* http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf. Interestingly, Helios is a voting system implemented using standard web servers and clients. However, it is explicitly intended only for "low coercion" elections. This makes Helios appropriate for electing the leader of an open-source software project or perhaps even for conducting Faculty Senate elections in a university setting. Helios was never intended for electing politicians to important offices.

[147] Sandler et al., *supra* note 51.

[148] Chaum et al., *supra* note 107, at § 1.

[149] Sandler et al., *supra* note 51, at 356.

[150] *Id.* at 358.

[151] Chaum et al., *supra* note 107, at § 2.

allow third parties to verify the tally and to challenge individual ballots, all without revealing how any specific voter cast a ballot.[152] Impressively, neither VoteBox nor Scantegrity is vulnerable *at all* to integrity attacks, assuming these systems are used and audited properly.[153] If only a handful of votes are flipped, then they may go undetected, but the odds of successful integrity attacks decline quickly as more votes are flipped. As such, most attempts to compromise ballot integrity will quickly degenerate to DoS attacks, and even those may be recoverable.

DoS for Scantegrity is identical to precinct-based optical scan—all the same O(*P*) attacks apply.[154] DoS for VoteBox is likewise still O(*P*), but VoteBox contains a number of data replication features that at least make it a constant factor harder.[155] In particular, for precincts with many VoteBox systems, they would be networked together, with each machine holding copies of the votes from every other machine.[156] An attacker would need to successfully attack *every* VoteBox machine in order to destroy the records of an election.[157] Scantegrity, by virtue of the paper ballots, is more robust against electronic tampering.[158] However, there are still only O(*P*) ballot boxes, themselves subject to physical tampering. In the end, while the specific attacks would be quite different, VoteBox and Scantegrity both have O(*P*) DoS vulnerabilities, allowing us to reasonably conclude that neither has a decisive advantage in this respect.

The cryptography in VoteBox and many other end-to-end systems generally relies on a notion of "election trustees" who hold "shares" of cryptographic key material and must collaborate together to tally and decrypt the votes.[159] Several O(1) confidentiality attacks exist if all the trustees collude together.[160] At that point, they could decrypt any individual ballot (violating confidentiality), learning how a specific voter

---

[152] *Id.* at § 4.8.

[153] *Id.* at § 5; Sandler et al., *supra* note 51, at 361–62.

[154] Chaum et al., *supra* note 107, at § 5 ("In our threat model, an adversary could be any party, including a voter, pollworker, or election official. The goal of the adversary is to attack the integrity of the election or exert undue influence over a voter. We do not consider attack vectors applicable to all voting systems, such as denial of service attacks, given that these attacks and countermeasures are not unique to Scantegrity II.").

[155] Sandler et al., *supra* note 51, at 353–59.

[156] *Id.* at 354–55.

[157] *Id.*

[158] Chaum et al., *supra* note 107, at § 1.

[159] *See, e.g.*, Sandler et al., *supra* note 51, at 361–62.

[160] Cryptographic key sharing mechanisms can be configured to require *every* share-holder to participate to perform a computation, or "threshold" schemes can be used that require some *k* out of *n* participants. If at least one trustee is honest (or, with threshold schemes, if a quorum of colluding trustees cannot be formed), then the system is secure. A malicious trustee could potentially conduct an O(1) DoS attack against the election by simply refusing to participate, and thus preventing the decryption of the election totals, but this would be impossible to do anonymously. Regular criminal penalties for this sort of behavior would hopefully provide the necessary deterrence.

cast his or her vote. However, they would be unable to delete ballots from the bulletin board, as voters would be able to detect the absence of their ballots.[161] They could perhaps add additional ballots, but these would need to have corresponding entries in poll books.[162] Ultimately, preventing ballot-stuffing attacks, in any voting technology, relies on having good records of whether a voter has or has not cast a vote, along with audits of these records for consistency with the number of cast ballots.[163] Scantegrity places all of this trust in a central election administrator.[164] If corrupt, a Scantegrity election administrator could violate the confidentiality of every ballot—an O(1) attack. (Generalizing Scantegrity to have a set of trustees rather than a single trusted election administrator would be a straightforward extension to the system.)

VoteBox has one additional O(1) DoS vulnerability: the destruction or loss of trustees' cryptographic key materials.[165] While key shares could be copied or backed up, this process would require careful design. Scantegrity is not vulnerable to a comparable attack because its paper ballots are always human readable and can be tallied using traditional scanners or by hand.

An important concern with VoteBox, Scantegrity, or any other end-to-end crypto voting system is what must happen if a fault is found.[166] What should the proper procedure be if a voter can prove, beyond any doubt, that his or her ballot was not included in the final tally? How many voters must provide such proof before the election results are called into question? Ultimately, end-to-end crypto voting mechanisms provide a great way of proving that an election was done properly.[167] Resolving errors, omissions, or fraud, once they are shown to exist, is likely to be a more labor-intensive process.

An intriguing issue for cryptography-intensive voting systems like VoteBox and Scantegrity is the issue of the strength of the cryptosystem itself. Modern cryptography rests on the computational difficulty of solving a number of "hard problems" such as factoring very large numbers. What happens if and when a future cryptographer invents an effective attack against the cryptography? A breakthrough like this would have ramifications well beyond the world of elections. Certainly, there would be a period wherein older broken cryptographic algorithms would need to be replaced

---

[161] Sandler et al., *supra* note 51, at 352–53.

[162] *Id.* at 350.

[163] *See generally* Daniel Sandler & Dan S. Wallach, *Casting Votes in the Auditorium*, 2 USENIX/ACCURATE ELECTRONIC VOTING TECH. WORKSHOP 1 (2007) (identifying the audibility of elections as a significant issue in electronic voting, and proposing an auditing infrastructure that provides "robust forensic documents" to verify the "global picture of critical election-day events").

[164] Chaum et al., *supra* note 107, at § 7.

[165] Sandler et al., *supra* note 51, at 361–62.

[166] *See* Benaloh, *supra* note 136 (providing an overview of ways to engage voters in "interactive proofs" to ensure that their own votes are cast as intended).

[167] Chaum et al., *supra* note 107, at § 8; Sandler et al., *supra* note 51, at 362.

with newer, replacement algorithms.[168] The main concern, for elections, would be that votes cast prior to the breakthrough could potentially be decrypted. (A similar threat occurs if the "trustees" collude, as described above.) A cryptographic failure, assuming it was known and corrected prior to the election, would not be usable to compromise election integrity or availability.

SUMMARY AND CONCLUSIONS

The table below summarizes the complexity analysis of attacking a variety of different voting technologies.

	Confidentiality	**Integrity**	**Denial of Service**
Vote-by-mail	O(*N*)—individual voters selling their votes O(*P*)—postal workers O(1)—election insiders	O(*N*)—individual voters selling their votes O(*P*), possibly O(1)—postal workers O(1)—election insiders	O(*N*)—individual voters selling their votes O(*P*), possibly O(1)—postal workers O(1)—election insiders
Paperless electronic	O(*P*)	O(1)*	O(1)*
Electronic + VVPAT	O(*P*)	O(*P*)	O(*P*)
Precinct optical scan	O(*P*)	O(*P*)	O(*P*)
Internet voting	O(1)	O(1)	O(1)
End-to-end crypto voting (Scantegrity)	O(*P*)—precinct tampering O(1)—corrupt election administrator	*impossible*	O(*P*)
End-to-end crypto voting (VoteBox)	O(*P*)—precinct tampering O(1)—trustee collusion	*impossible*	O(*P*) O(1)—trustee key loss

*These O(1) attacks may be partially mitigated using complex procedures described by Halderman et al.,[169] which could strengthen the systems from O(1) to O(*P*).

[168] *See generally* Halderman et al., *supra* note 71 (discussing integrating new voting technology with systems already in place while ensuring secured transactions).

[169] *Id.*

Based on a straightforward complexity analysis of different voting technologies, we can reach clear conclusions about their relative strengths and weaknesses. While no voting system is perfect, understanding the relative effort required to mount an attack is critical to allocating resources toward defeating these attacks. For example, if election officials are conducting a vote-by-mail election, then clearly they need to spend significant effort in their internal security procedures to detect and defeat the constant cost threat of insider attacks. Likewise, the constant effort attacks against Internet voting, and the lack of adequate remedies, provide more than sufficient justification to use other modalities for conducting elections. We do note that the Internet is useful for connecting precincts back to election headquarters, so long as it is not relied upon for election correctness.[170] Another consistent theme is that election registration procedures should never record the order in which voters appear, as this reduces the complexity of anonymity attacks across many different technologies. Of voting technologies presently on the market and certified for use in most states, precinct-based optical scanning systems appear to have the best resistance to security attacks, based on our complexity analysis. Future cryptographic end-to-end systems should be able to improve upon this, although it is an open question whether normal voters would find these systems to be usable.

[170] Sandler et al., *supra* note 51.