Michael Morisi
Comp 116: Web Security

Examining the Insecurities of the DRE Voting Machine

Abstract

As the world pushes further on into the digital age and as we leave behind the paperless society that previously existed, one key change being made is at the heart of the system of elections. As we hold more and more elections, and as time passes on and on, we are steadily phasing out the outdated system of paper ballots in favor of the more streamlined system of electronic voting machines. Not only do they make the voting process easier, voting machines also serve to make the process of counting ballots less arduous. However, this transition into the digital age has also naturally led to the possibility of malicious hackers seeking to exploit the burgeoning number of machines by manipulating the results, most notably visible these days in the ongoing FBI investigation of Russian influence over the 2016 Presidential election.

This paper will explore the myriad ways in which security experts have shown that voting machines can been taken advantage of by third parties, as well as the methods these third parties could potentially employ.

Introduction

Electronic voting machines seek to alleviate a much-publicized problem: counting physical ballots manually is arduous, time-consuming, and oftentimes imprecise. Purely electronic machines can be dated to the 1980s, where push-button direct-recording electronic (DRE) machines began to become both more widely accepted as well as commercially successful. DRE machines operate by storing recorded votes on physical memory in the machine. Some of them include features for sending recorded votes to a centralized location for counting, instead of having to physically remove the memory.

To the Community

This paper topic was selected because the ideas of election security have never been more prevalent. The idea of Russian interference in our most recent election has been a top story on the news for months now. Increasing public awareness and knowledge of the current state of our nation's electronic voting systems allows the general public to be better aware of what happens to their electronic votes after they are cast, as well as how their vote could potentially be exploited during the election process.

A Brief History of Paper Ballots

When a potentially imprecise method such as manually marking ballots is implemented, this comes with plenty of questions about the validity of the outcomes they produce. Paper ballots are often subject to inaccurate results in part due to some combination of human error in both counting and recording one's votes. One of the most infamous instances of the potential problems with paper ballots is the recount in Florida during the 2000 presidential election, in

which an initially reported Gore victory over Bush with a 0.5% difference in vote count triggered a recount mandated by state law, which ended up reversing the outcome and, by extension, the outcome of the election. This only happened due to a design flaw in the paper ballots used, as voters oftentimes wouldn't perforate completely through the ballot when casting a vote, leading to some ballots with unclear outcomes. In some cases, the unorthodox layout of the ballot actually caused voters to select the wrong candidate. This incident triggered a nationwide skepticism for the continued usage of a voting medium which seemed more antiquated by the day (Harrington).

The Rise of the DRE Machines, and the Emergence of Flaws

With the 2000 presidential election being a red flag for the negatives of the continued usage of paper ballots, the United States government updated the voting system standard regarding voting mediums in the years following. By 2002, the first state (Georgia) had begun to use DRE machines on a statewide basis (ProCon). Initially, confidence in the technology was high – in 1996, Dr. Michael Shamos of Carnegie Mellon University released a challenge with a $10,000 prize which would be awarded to someone who was able to undetectably tamper with a "well-designed" DRE machine (Shamos). The year 2002 also brought the Help America Vote act, which sought in part to improve the voting process by eschewing outdated punch card methods in favor of modern systems, mandating that states upgrade any voting systems currently in place. The nation was tired of the old and was ready for a breakthrough in voting technologies to come.

In 2003, however, the cracks in the budding DRE empire became apparently when Avi Rubin and Dan Wallach of Johns Hopkins University published a paper lambasting the security, or lack thereof, of the commonly used Diebold-brand DRE machines implemented around the United States. Rubin and Wallach described several flaws and exploits in DRE machines, including voters being able to cast multiple ballots without a trace, as well as administrative abilities being available to regular voters. The Diebold system uses smartcards to authorize voters as a form of two-factor authentication (the other factor generally being an ID card). The paper states that the use of smartcards in the Diebold system is easily exploited, with Rubin's team discovering that there isn't actually any truly secure authentication of the voter's smartcard by the voting terminal, and therefore it's possible to create homebrewed smartcards. A homebrewed admin smartcard would give an attacker the ability to view partial results or even stop the vote entirely. Rubin and his colleagues also cited the susceptibility of the machines to being tampered with by a present malicious attacker, who could be working as a janitor or a poll worker, who could show up with a stack of homebrewed smartcards, which the system recognizes as perfectly valid, and falsify a series of votes (Rubin).

More Issues Arise

From there on, more incidents around the United States emerged as the 21st century progressed regarding the issues surrounding DRE machines. The 2004 general election in North Carolina lost over 4000 votes cast using DREs because manufacturers mistakenly claimed they held up to 10,500 votes when in reality they only stored 3005 (ProCon).

Furthermore, at this point in time, security experts began to truly test these machines with more rigor and intensity. In 2005, the Hursti Hack, so named after programmer Harri Hursti, was a well-publicized live demonstration where Black Box Voting Inc. were successfully able to infiltrate a Diebold voting machine, a DRE machine used by up to a quarter of American voters, alter vote totals in a sample Leon County election, and leave no traces, all by modifying the contents of the machine's memory card (Goldfarb). Hursti did this by modifying the portion of the software which outputted the voting results, as well as the central vote tabulator. The Leon County Election Supervisor would later go on to say that if the vote was a real one, he would have approved the election results. A later paper about the Hursti Hack written by scientists at UC Berkeley stated that "[Hursti] needed no passwords, no cryptographic keys, and no access to any other part of the voting system, including the GEMS election management server" (Wagner). The same paper claimed that all bugs in the Diebold systems were very easy to fix, essentially boiling down to fixing bugs in code that shouldn't have existed in the first place and enforcing a stricter coding methodology (The Berkeley scientists claimed that the machine's programmers used typical commercial practices instead of more rigorous, security-minded ones), as well as not storing actual source code on removable memory cards found in the machine.

In 2011, yet another Diebold exploit was found, whereby a device that cost a hair over 10 US dollars in parts could be used to remotely hack a Diebold machine when installed. Once this man in the middle is set up using the device, the malicious third party can remotely manipulate results with no trace left in the software by intercepting and modifying selections made by voters after they had already made their choice. Therefore, although the vote would be changed, the Diebold machine would still display the correct feedback to the unsuspecting voter. This device, according to those who made it at the Vulnerability Assessment Team at Argonne National Laboratory, "required no modification, reprogramming, or even knowledge, of the voting machine's proprietary source code" (Friedman). The Argonne team mentioned that inserting the device was as simple as picking a rudimentary lock on the machine, because all the machines use the exact same copy of the same key. The security risk is massive and obvious – one master key to open all the machines opens up an extremely wide avenue for exploits.

The 2016 Election and Voting Security Today

While the 2008 United States presidential election went off mostly without a hitch in terms of security flaws, and the main problem in the 2012 election was a few malfunctioning machines, the 2016 election has been widely publicized for the question of the extent of Russian tampering on the voting process and results. The American public was made aware of Russia's spearheading of an influence campaign against the Democratic party, to the point where incumbent president Barack Obama resorted to using the "red phone" hotline to Russia to give Vladimir Putin a warning to cease and desist all interference. However, evidence has surfaced which points to Russia having hacked into voting systems in at least 39 states before the election, with the Illinois board of elections being the first to learn of the influence when unauthorized data was monitored leaving their network. Given that 43 of the 50 states used

DRE machines that are at least 10 years old in the 2016 election, it also points to Russia targeting our dated, easily exploitable voting hardware (Ward).

Defenses

In November 2017, Matt Blaze of the University of Pennsylvania gave a testimony to Congress to discuss the current largest risks and vulnerabilities in the elective process, specifically the massive weaknesses in DRE machines. Blaze lays down three recommendations which he feels are imperative to tightening up election-time security in the nation:

1. Substitute paperless DRE machines for options which leave the voter with an artifact of their vote (e.g. optical scanners which scan a marked ballot)
2. Employ statistical "risk limiting audits" after every election to detect malfunctions or attacks
3. Employ stronger resources, training, supervision, and infrastructure to voting officials at every level to ensure stability in the process

Blaze cites the DRE machine's proven track record as being an unreliable, easily exploited machine which, when tampered with, leaves no trace of the attacker, nor record of what was on the machine prior. Perhaps even more importantly, Blaze claims that the current state of electronic voting in the United States is particularly vulnerable to an attack from an adversary on the scale of a nation-state. He cites a hostile nation-state's ability to disrupt an election coupled with a nation's expanded resources and intelligence services makes influencing an election's outcome trivial, especially when the United States depends on out-of-date technology (Blaze). Therefore, to improve the security of these machines, it's imperative that the manufacturers of DRE machines adhere more closely to strong security principles (as crazy as it is that they haven't been consistently doing so already).

Conclusion: Looking Forwards in the Electronic Voting Process

Naturally, if the United States wants to ensure the legitimacy of votes obtained using voting machines, the first step is to eliminate DRE machines. Not only is their history of being tampered with extensive and detailed, but the ability to tamper one without leaving a trace is arguably more disturbing. Fortunately for the public, and as indicated by both the Blaze testimony and the massively publicized Mueller investigation into Russian election tampering, awareness of the issues of voting security have never been higher. Looking back at the myriad occasions in which a consistent lack of mindfulness for best security practices has potentially jeopardized the security of our voting process, it would be the best for our nation if we can use those mistakes as lessons for the future, and finally reclaim legitimacy and faith in one of the most important processes in the nation.

Works Cited

Blaze, Matt. “HEARING ON CYBERSECURITY OF VOTING MACHINES.” 29 Nov. 2017.

Friedman, Brad. “Diebold Voting Machines Can Be Hacked by Remote Control.” *Salon*, Salon.com, 27 Sept. 2011, www.salon.com/2011/09/27/votinghack/.

Goldfarb, Zachary. “As Elections Near, Officials Challenge Balloting Security.” *The Washington Post*, WP Company, 22 Jan. 2006, www.washingtonpost.com/wp-dyn/content/article/2006/01/21/AR2006012101051_pf.html.

Harrington, Rebecca. “Florida Was Almost Too Close to Call - Here's What Happened in the 2000 Recount and How It Nearly Happened Again.” *Business Insider*, Business Insider, 8 Nov. 2016, www.businessinsider.com/could-florida-recount-happen-again-how-presidential-election-2000-2016-11.

“Historical Timeline - Voting Machines.” *ProCon.org*, votingmachines.procon.org/view.timeline.php?timelineID=000021.

Rubin, Avi, et al. “Analysis of an Electronic Voting System.” *IEEE Symposium on Security and Privacy*, 27 Feb. 2004, avirubin.com/vote.pdf.

Shamos, Michael. “The DRE Tampering Challenge.” *The DRE Tampering Challenge*, 1996, votingmachines.procon.org/sourcefiles/tamperingchallenge.pdf.

Wagner, David, et al. “Security Analysis of the Diebold AccuBasic Interpreter.” 14 Feb. 2006, web.archive.org/web/20161202140146/https://www.supportthevoter.gov/files/2013/09/VSTAAB-Security-Analysis-of-Diebold-AccuBasic-Interpreter-2006.pdf.

Ward, Alex. “Russia Hacked Voting Systems in 39 States before the 2016 Presidential Election.” *Vox*, Vox, 13 June 2017, www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions.