Examining the Security Risks of Voting Machines within the United States

Kenneth Slaby

COMP 116: Introduction to Computer Security

December 13, 2017

Introduction

Modern democratic societies rely heavily on a strong system for the processing of votes by the voting population. In the digital age that we find ourselves in, the methods for counting votes have moved from the pen and paper style system to a mostly technological one. While using technology as a method of counting votes has dramatically increased the speed and accuracy in which we count them, it does pose certain risks. With the accusations of hacking from Russia over the recent US 2016 election, many people started to take a critical look at our election mechanisms. Thus, an important first step was to examine the security faults in the software and hardware of the voting machines, understand the threats they pose to voting integrity, and discuss ways for how to prevent those issues as a whole.

Abstract

In this paper, we will discuss the results of the examination of the security faults in the voting machines themselves, their software, and how to better protect the democratic system from hacking on election day. For each of these, we will discuss the issues in detail as well as propose potential solutions that could be implemented for the highest impact for national safety.

To the Community

One of the biggest parts of election security comes on election day. Every year in the United States, millions of people show up at the election polls in order to vote in their president elect. Polling places are packed, poll workers assisting many voters with their tasks. Their systems for securing votes and ensuring that the individual has their own privacy gives them a false sense of security. While to an outside viewer, these methods appear to be secure and infailabe, systematic issues have been present across the board for many years. While many of the people who take steps into the voting booth will be mostly unaware by these present issues, it is the few malicious people, who given the proper tools and knowledge of the machines, can

not over destroy the integrity of their vote, but possibly the integrity of the entire station. Every person who had voted there that day, and if on a large enough scale the election as a whole could be compromised by a well armed attacker. Thus, we must learn to protect ourselves from these attacks before they can be committed by thoroughly examining the process as a whole as well as the security of the tools used by the masses.

Supporting Information

These machines, which have been used for many years, have consistently had flaws since their creation. There has been the possibility that they have been insecure and unsafe for many years before their current revelations. From their inception, the digital voting machines were untrusted by the masses.[1] The machines were seen as unsafe ways that prevented recounts in cases of failure; that they were not infallible, and that when they did fail there was no way for the information that was lost to be recovered. Many people were concerned at the development of these digital systems, despite comments by Ted Selker, assuring people that "the paper trail is much more prone to fraud than the electronic trail," this distrust remained present.[2]

For years, it appeared that this distrust was unwarranted, as surely an increase in technology would secure the process overall. The increase of digital methods from the old paper methods should spell out a faster and more stable procedure, but in reality, it has only made the insecurities in the process become more apparent. As time has gone on, and as the general public has increased in it abilities for understanding technology at a more critical level, we have seen these inadequacies within all of our technology more often. The digitalization of the voting process was not absolved of these issues. It has been the general public who has come to find issues with these machines, not the government agencies and other organizations (such as the

[1] Eugenie Samuel Reich and Celeste Biever, "Analysis: The great American e-voting experiment." *NewScientist.* 16 October, 2004. https://www.newscientist.com/article/dn6523-analysis-the-great-american-e-voting-experiment/.
[2] Ibid. At the time of this comment, Ted Selker was a Professor at MIT.

Independent Testing Authority). In September of 2017, DEF CON put on a 'Voting Village,' where they were able to secure 25 different kinds of used voting machines. Over the course of just three days, the attendees were able to hack into every single one of them: "By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems."[3]

This 'Voting Village' was an eye opening for the lawmakers of the US, whom on the 29th of November, 2017, listened to a report of the events from Matt Blaze, who was one of the organizers of the 'Voting Village.' Matt's ultimatum to the House Subcommittee was damning of the entire situation, and in his own words, "Paperless DRE[4] voting machines should be immediately phased out from US elections in favor of systems, such as precinct-counted optical scan ballots, that leave a direct artifact of the voter's choice."[5] These systems, which were the primary systems present at the Voting Village, have proven to be inherently insecure. Not only are many of their actual operating systems out of date (which will be shown later in further detail), but their general insecurity for the same reasoning as their initial distrust compromises their reliability. That should a machine that behaves in such a manner as a DRE, some of which operate without leaving a paper trail at all, be compromised, there would be almost no way to know that the machine had been tampered with, as there are little to no artifacts of the tampering that would be present. According to Matt, these machines can be affected in numerous ways, including the removal of information from log files, the tampering of the material

---

[3] Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, Jeff Moss. "DEF CON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure." *DEF CON.* September 2017.https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

[4] Ibid. 5. "Direct Recording Electronic (DRE) Voting Machines – DRE machines are special-purpose computers that display ballot choices to the voter (based on the ballot definition) and record voter choices."

[5] Matt Blaze. *US House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs Hearing on Cybersecurity of Voting Machines.* 29, November, 2017. 2 https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf

displayed to the voters, and the actual destruction of internal memory of the machine.[6] In the end, these machines are not worth the time of the voting public, and we must find or create a new suitable alternative in order to secure our voting information for the day of the next election.

In order to better illustrate the severity of the issues at hand, we must examine the direct evidence that came out of the September 2017 DEF CON conference. As previously mentioned, of the 25 available machines to tamper with, not a single machine escaped the brilliant minds of the conference attendees. One of the most dramatic of the issues discovered came from the AVS WINVote DRE,[7] which was one of the biggest offenders from the conference. The WINVote system is a "touch-screen voting terminal equipped with a wireless local area network (LAN)."[8] To the untrained eye, it is just another voting system; but to the hackers at DEF CON, they aptly noticed that the WINVote operating system is running Windows 2000. This, in combination with the fact that it creates a local network that is "completely unprotected,"[9] leaves the machine wide open to various attacks. Armed with this knowledge, the DEF CON attendees were able to completely take over the system, utilizing a well know buffer overflow vulnerability with Windows 2000 machines.[10] This vulnerability, which was present on all the WINVote machines, could allow any person with the proper knowledge of buffer overflows complete control over the system, causing a major disruptions on election day.

The AVS WINVote was not the only machine with well known security vulnerabilities. Many of the others, including the Diebold ExpressPoll 5000 faced similar problems as their WINVote counterpart. Running a older version of Windows CE 5, the Diebold ExpressPoll 5000

---

[6] Ibid. 8-9.
[7] Blaze. "DEF CON 25". 7. Software version 1.5.4 / Hardware version N/A.
[8] *Advanced Voting Solutions (AVS) WINVote (and WINScan). VerifedVoting.* n/d. Accessed 10, December, 2017. https://www.verifiedvoting.org/resources/voting-equipment/avs/winvote/
[9] Blaze. "DEF CON 25." 16.
[10] CVE-2003-0352. *MITRE Corporation.* 10, October, 2017. Accessed 10, December 2017. https://www.cvedetails.com/cve/CVE-2003-0352/ "Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms."

machines default to an easy to find default password and have no input validation.[11] What information that they contain can be easily reconfigured by a malicious attacker who has access to its unprotected USB ports, which at the conference the participants were able to completely shutdown the system.[12] Like the WINVote, these issues, which now have become public knowledge, could bring complete devastation if not addressed by the next election.

Action Items

These problems have been present among our voting systems for years, and it is only now that we are starting to take a critical look at their root causes. Inorder to solve these issues, it is imperative that we solve some of their underlying causes first, in addition to ensuring that we secure the integrity of the machines before election day. Part of ensuring their integrity before we even received the machines is to create fail safes on the manufacturing side. Currently, many of the machines have their important internal components made overseas, which does lead to the potential for tampering prior to them even setting foot on American soil.[13] While manufacturing in the United States has left for the most part, ensuring that above all else these manufacturing plants are highly scrutinized, or the plants making the key pieces for the machines are located within the United States, would be a large first step into solving this problem.

Many of the issues that were found among these voting machines were because of outdated software. Ensuring that the software of these machines stays up to date with modern technology is critically important and would be a relatively straightforward way to solve some of the more well known issues. The problem then becomes: “How do we ensure that the software

---

[11] Blaze. “DEF CON 25.” 13.
[12] CVE-2008-4609. *MITRE Corporation.* 28 September, 2017. Accessed 10, December 2017. https://www.cvedetails.com/cve/CVE-2008-4609/
[13] Ibid. 15. “But via a supply chain originating overseas, voting equipment and software can be compromised at the earliest of stages in manufacturing process. For example, foreign actors could design or plant a virus in software, memory, or even a small microchip that could affect an entire make/model of voting machine, theoretically allowing them to be compromised in one coordinated attack.”

updates are often enough and secure enough to avoid issues in the future?" Additionally we need to ask: "How do we maintain a sense of responsibility in the manufacturers that are creating the physical hardware, and the software developers creating the digital databases and information? Going off of Matt Blaze's analysis, a clear and easy route would be simply to make the software open source, which would allow others to help discover issues before they even become real. This way, its becomes a job of the masses to help ensure our voting integrity, not that of a smaller group of individuals who might miss and issue because they were not able to expand their thinking in the same way a large group can.

Conclusion

Being a part of a democratic system will have its ups and downs. We must do what we can in order to better defend ourselves from all possible sources of attacks, both external and internal. Our voting system is in peril, in danger from the inability for democracy to keep up with technology. The issues presented in this paper are not insolvable, but until we take action as a nation to secure our fundamental structure of voting, we face the dangers of malicious attackers every time we step into the voting booth. The results from this 'Voting Village' will hopefully shed new light on many issues that were previously overlooked with our election system. By the time of the next election, the United States will likely have seen a dramatic increase in its electoral security systems across the nation.

References

Advanced Voting Solutions (AVS) WINVote (and WINScan). VerifedVoting. n/d. Accessed 10, December, 2017. https://www.verifiedvoting.org/resources/voting-equipment/avs/winvote/

CVE-2003-0352. *MITRE Corporation.* 10, October, 2017. Accessed 10, December 2017. https://www.cvedetails.com/cve/CVE-2003-0352/

CVE-2008-4609. *MITRE Corporation.* 28 September, 2017. Accessed 13, December 2017. https://www.cvedetails.com/cve/CVE-2008-4609/

Eugenie Samuel Reich and Celeste Biever, "Analysis: The great American e-voting experiment." *NewScientist.* 16 October, 2004. https://www.newscientist.com/article/dn6523-analysis-the-great-american-e-voting-experiment/

Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, Jeff Moss. "DEF CON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure." *DEF CON.* September 2017.

Matt Blaze. *US House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs Hearing on Cybersecurity of Voting Machines.* 29, November, 2017.