Zachary Goldman

12/13/2017

Comp116: Security

The Security of Elections

ABSTRACT

In an age of digitalization, most everything that was previously done with pen and paper can be done on a computer screen. As the result of this, there's been a push to add voting to the list of things we do on a computer screen. Many states have already implemented electronic voting booths, but this innocent idea can lead to dire consequences. Voting booths as they exist now have been shown to be extremely vulnerable, and those issues have not been addressed. The goal of this paper is to explore the tradeoffs associated with voting booths in terms of cost, accessibility, and security. Although there are certainly benefits to having electronic voting booths, they are ultimately too great a risk due to the costs and importance of maintaining a secure system, even with something so seemingly basic as a digital voting booth.

INTRODUCTION

Voting machines have begun to creep into the mainstream as they become more integral to the infrastructure of the election process. The rise of voting machines can be attributed to the Help America Vote Act (HEVA) which came into place after the 2000 presidential elections, when the punch card voting machines malfunctioned in some districts, making the results of the elections difficult to determine. This type of platform eschews traditional pen-and-paper ballot voting mechanisms in favor of a machine that wouldn't look out of place in an arcade. The machine is shrouded beneath a booth designed to prevent any supervision of the voter to

preserve the anonymity of the voter and therefore the integrity of the vote. There are two main benefits to these platforms. Voting machines are able to randomize the order that candidates are presented in, which can eliminate voter biases such as voting for whichever option appears first when the voter isn't familiar with the context of the choice (Sabato 2009). The other benefit of these machines is that they automate the vote-counting process. Rather than have a committee of people sort through each individual ballot, tallying votes one-by-one, these machines can keep an ongoing count as each voter votes. Theoretically, these benefits should combine for more accurate voter results, eliminate human error, and save time and money. As far as United States elections go, this is the only electronic voting mechanism in place right now – the other implementations this paper will discuss have only been suggested. Multiple different types of booths are in use in U.S. elections, such as the AccuVote-TSx, Sequoia AVC Edge, and the ES&S iVotronic (Blaze et al. 2017). Most voting systems in place right now are DRE systems

TO THE COMMUNITY

Electronic voting booths carry a number of security concerns despite the apparent benefits. Although this method of voting is the most similar to the traditional paper ballot among the platforms this paper will discuss, voting booths have been exposed as vulnerable on numerous occasions. Even if the booth is not connected to anything wirelessly, the voter is left in private with the machine for an extended period of time, during which they could access the hardware. DEFCON held a 'Voting Village' in July of 2017 where, in response to attacks on our voting process, including a successful cyber attack by Russians on our voting process, a number of hackers were tasked with exposing the vulnerabilities in election machines (Blaze et al. 2017).

The results, which were published in a detailed report after the event, paint a grim picture for the prospects of voting machines.

In the Voting Village, participants attempted to break in to the AVS WinVote, a voting machine that had been in use as recently as 2014. The machines are connected to Wi-Fi and have their own IP addresses, so hackers were able to attack them remotely with relative ease. It only took Dutch researcher Carsten Schürmann minutes to gain access to the system, utilizing tools such as WireShark and Metasploit. The vulnerability he exposed had been documented as early as 2003 (CVE-2003-0342). This vulnerability was particularly concerning, as usernames and passwords were stored in a file in plaintext. This allowed him to obtain administrator privileges on the machine, giving him the ability to run code and change votes. There were also USB ports exposed on the machine, making an attack trivial. The extreme vulnerability of these machines cast doubt on the integrity of any election between 2003-2014.

The DEFCON study came with one important caveat – the Voting Village participants did not have access to the backend of the voting systems. A number of the machines examined had functionality that allowed them to transmit the vote counts over a network to a central database. This is where the results of the voting are stored, and the most likely target of the Russian cyberattack (Blaze et al. 2017). The exact way that the backend is set up is unknown, and varies by machine, but they're likely subject to data injection via man-in-the-middle attacks using a proxy. Transmitting voting data remotely leaves opportunity for a number of vulnerabilities to intercept and inject data, compromising the confidentiality, integrity and availability of the voting data that would be used to determine the outcome of elections.

A number of other machines still in use today were examined, and there were a number of common problems with the machines. Limited physical security was a vulnerability many of the machines had in common, as the hardware for multiple machines could be accessed with a screwdriver or a flash drive. A number of vulnerabilities from the OWASP top 10 were present, such as Broken Authentication (A2) and Using Components with Known Vulnerabilities (A9) (Blaze et al. 2017). What's perhaps the most troubling about this is that some of these findings were also detailed in the landmark EVEREST study conducted a decade ago. Both studies examed ES&S systems, as well as AV-TSx, and many of the vulnerabilities had not been rectified (Aviv et al. 2007).

The EVEREST study examined a wide variety of voting systems, but still managed to find critical flaws in each and every one of them. There were rampant issues with authentication, input validation and sanitation, hardware security, cryptography, and others (Aviv et al. 2007). Each machine examined had its own unique share of vulnerabilities, and EVEREST detailed several different methods which could be used to completely change the voter data, or prevent voting from taking place at all (Aviv et al. 2007). The variety of issues illustrates one of the core issues at play. Given the sheer number of vulnerabilities that have already been documented, and remain unsolved, the tradeoffs these voting platforms necessitate must be analyzed. Although voting booths undoubtedly provide benefits to the election process, there's a number of important factors to take into account when considering their use.

Given the sheer amount of vulnerabilities an election machine has, making them completely secure is a difficult task, if at all possible. Features that would likely need to be included, in addition to standard security practices (e.g. input validation, access control, least

privilege) would include draconian measures like the search of each voter as they enter the premises, taking the machines completely offline, manually transporting the hard drive to a secure database to upload each individual vote as they come while simultaneously building the machine in a chassis that would be impossible for a voter to access, incorporating a cryptographic checksum along with 2FA to validate the validity of each vote, among others. What this eventually approaches is a process that's very similar to pen-and-paper voting but with more expensive upkeep, but with a higher maintenance cost, and significantly more accessibility barriers to the voter.

Even if the unrealistic goal of 'perfect security' were to be abandoned in place of the more achievable 'relative security,' there are other concerns that must be addressed. The number of different types of voting machines employed raises real concerns about how to secure them. If the status quo remains, and the government continues to employ multiple different types of voting machines, the cost (time, money, opportunity) of securing each one is multiplied by the number of different systems employed. This would necessitate a significant amount of resources that could otherwise be saved. To minimize this, the government could mandate that the machine used be standardized so that only one type is employed. In theory, this would mean that if you secure one machine, you secure them all, so the cost would be severely reduced. However, the tradeoff here is significant. As securing one would secure all of them, exposing a vulnerability in one machine would expose a vulnerability in every single voting machine. This would raise the burden of security dramatically, perhaps approaching the draconian measures mentioned above, in order to ensure that the election was administered properly.

It's also important to consider that these machines are only ever used in two-year intervals. Attackers would have two years to uncover a vulnerability, and if the machines are standardized the target is more clearly identified, but since they're only ever used one day in a two-year span, there would be no time to respond to an incident. Keeping them secure would require a herculean effort by a team dedicated to testing them constantly. So, while the road to improvement for the existing machines is definitely available, there are a number of tradeoffs with no easy answers, and a significant level of investment required in all of them.

ACTIONABLE ITEMS

There are a few things that people can do to ensure the integrity of their vote. First, if you plan on voting, reach out ahead of time to the directors of your polling place to see how they'll be administering the voting process. If voters are given the option between electronic voting and paper ballots, elect to use paper ballots. If there will only be electronic voting, request paper ballots; look up what type of machines your district will be using, and write to your Representative and your Governor requesting the suspension of their use. This is a large-scale national security risk, but every vote you can preserve makes a difference. Additionally, around half of states don't conduct post-vote auditing, one of the best ways to ensure confidence in results (Barrett, 2016). If you live in one of these states, write to your elected officials demanding a system be put in place in order to help maintain integrity in the election results. Without these audits, vote totals are not checked against the amount of people who actually voted, so injecting votes becomes trivial.

CONCLUSION: A BETTER WAY!

The findings above raise an important question when considering the future of our electoral process. Ideally, there would be a way to vote that wouldn't require much investment, continuous upkeep, be totally secure, and not hinder the accessibility to voters. In reality, such a voting method exists, and the United States has employed it for a very long time: a pencil and a ballot sheet. Although a voting machine does provide some benefits, there are significant tradeoffs that do not seem worth it. Voting machines themselves provide a benefit for the electoral system's infrastructure, but as they are now, they posit a huge security threat. When voting systems were first created, this was not as much of a concern, but recent elections have demonstrated why that mindset must change. However, securing these systems places a significant burden on the voting infrastructure, and may come at the cost of voter accessibility. It stands to reason that the best option available is the one that's proven trustworthy time after time for hundreds of years. Electronic voting systems are not software independent, and rely on public networks to transfer data. The best example of a strongly software independent voting machine is a paper ballot (Rivest 2016).

WORKS CITED

Aviv, Adam, Cerny Pavol, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, and Matt Blaze. 2007. “Security Evaluation of ES&S Voting Machines and Election Management System.” Department of Computer and Information Science, University of Pennsylvania. https://www.eac.gov/assets/1/28/EVEREST.pdf.

Blaze, Matt, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss. 2017. “DEFCON 25: Voting Machine Hacking Village.” DEFCON. https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

Sabato, Larry J. 2009. “WHO’S ON FIRST? Does the Ballot Order of Candidates Make a Difference?” University of Virginia Center for Politics. http://www.centerforpolitics.org/newslet_909cb.html.

Rivest, Ronald L. 2016. "Auditability and Verifiability of Elections" ACM-IEE Talk. https://people.csail.mit.edu/rivest/pubs/Riv16x.pdf

Barrett, Brian. 2016. "America's Electronic Voting Machines Are Scarily Easy Targets" Wired Magazine. https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/