Safeguarding U.S. Voter Information

Rebecca Alpert
December 10, 2017

Abstract

While they have been hailed as a way to improve accessibility for voters, electronic voting systems have been controversial for years. Implemented in countries like Canada and Estonia, their use in the United States has generated headline after headline in recent months.

On June 5, 2017, *The Intercept* published a top-secret NSA report detailing a Russian cyberattack on a U.S. voting software supplier and spear-phishing attempts on local election officials prior to the 2016 election. The attack focused on voter databases rather than touch-screen voting interfaces. However, attacks on such software have very real potential to disrupt normal voting in the U.S.

Regardless of where your politics lie, ensuring the integrity of U.S. elections should be of paramount importance. In this paper, I will give a brief overview of electronic voter databases, detail common vulnerabilities, and discuss actions that government officials can take to safeguard the privacy and security of voter data in the future.

Introduction

State voter databases are used to record who may vote in an election and have been available electronically since 2002. The Help America Vote Act (HAVA) of 2002 required states to create statewide voter registration databases. However, the act left details on

technology and implementation to the states. As a result, these databases vary widely from state to state.

Online voter registration is touted as more accessible and convenient, cheaper to process, and more accurate than previously used paper-dependent voting. However, election officials often lack funding or IT support, and many election officials and election-related contractors seemingly lack knowledge of basic cybersecurity best practices. Many recent data breaches have made it clear that our systems are vulnerable to data breaches or malicious attacks from foreign actors.

Fortunately, once we know what the vulnerabilities are, we can take concrete steps to harden them against attack. The goal of this paper is to outline vulnerabilities in U.S. voter databases and steps we can take to mitigate them. However, funding and IT support will be critical to successful implementation of mitigation.

To The Community

Database systems throughout the U.S. are vulnerable to attack and need to be more secure to ensure the integrity of U.S. elections. Compromised voter databases can be used to block voters, cause disruption, and undermine confidence in the vote. This paper aims to explain vulnerabilities in our voter database systems and concrete steps we can take to harden them against attack.

However, hardening our systems will require funding and IT support, which election officials often lack. Your help is needed to make safer systems a reality -- U.S. citizens need to come together and make it clear to our representatives in Congress and the House that improving the security of our voter databases is a priority.

Background

On June 7, 2016, voters alerted Riverside County District Attorney Michael Hestrin that they hadn't been able to vote in the California presidential primary. It turned out that some voters' registration information had been changed without their knowledge -- which prevented them from voting -- by hackers using the voters' private information. While there were no system logs, which could have been used to help identify who had accessed the accounts, cybersecurity officials who have learned about the attacks have suggested that Russia may have used it as a test run for their later attacks on the U.S.

Russia's later attacks on the U.S. 2016 presidential election were highly publicized. The attacks consisted largely of attacks on election officials and VR Systems, a manufacturer of Internet- and Bluetooth-connected devices used to maintain voter rolls. Attacks began with phishing attempts on VR Systems, a few of which succeeded and allowed Russian hackers to obtain login credentials for VR Systems employees.

Hackers then launched a second phishing attempt on government employees that looked as though they were from VR Systems, and delivered malware disguised as a Microsoft Word file. Opening the file would have allowed hackers to steal data -- and it's still unclear exactly what data may have been stolen. Based on these events, it's clear that U.S. voter database infrastructure is vulnerable to attack and could potentially disrupt U.S. elections.

Common Vulnerabilities

Due to lack of funding and IT support, voter database infrastructure is often old. The Brennan Center for Justice at New York University School of Law, a non-partisan public

policy and law institute that focuses on the fundamental issues of democracy and justice, estimates that 41 states are using databases created at least 10 years ago. Some even use old software like Windows XP or Windows 2000, which is no longer supported and vulnerable to attack.

In addition, access to databases is not properly secured. On July 18, 2017, cyber resilience startup UpGuard published a report on the largest leak of U.S. voter data to date. They found that Deep Root Analytics, a GOP analytics company working for the Trump campaign, stored voter data in a public Amazon Web Services S3 bucket. This leak exposed the sensitive personal details of over 198 million American voters -- 61% of the entire U.S. population. This isn't an isolated problem -- just a few months later, UpGuard staff also discovered a publicly accessible S3 bucket owned and operated by a voting machine company which exposed information on 1.8 million voters in Chicago.

Recent research has also revealed that voter registration websites are vulnerable to identity theft. In many states, these sites allow voters to register or allow previously registered voters to change their personal information. They often use sensitive information to confirm a voter's identity. However, that information may have been compromised in security breaches, such as the recent Equifax data breach, or by other means.

A new study published in September by Latanya Sweeney, Ji Su Yoo, and Jinyan Zang in the *Journal of Technology Science* found that websites for 35 states and D.C. in 2016 were vulnerable to these identity theft-related attacks. The researchers used names, dates of birth, addresses, driver's license numbers, and Social Security numbers obtained from data

brokers, data breaches, vulnerabilities in the way some states' driver's license numbers are encoded, and state voter lists to compromise accounts. The data could be used to change voter addresses in order to make voters ineligible to vote, allow attackers to submit absentee ballots in the names of legitimate voters (which would also prevent legitimate voters from voting in person), or change party affiliation to prevent voting in a primary.

Finally, workstations are not locked down and employees are uneducated about best practices for cybersecurity. For example, phishing attacks and malware were used in the Russian cyberattacks during the 2016 election. Furthermore, in some cases, employees transmit sensitive data in plain text across the Internet.

In October, anti-Trump citizens' group Indivisible Chicago posted documents illustrating glaring security problems in the administration of the Crosscheck interstate data-sharing program. Usernames and passwords were transmitted in plaintext via email and the program used an insecure, unencrypted FTP server for upload of state voter data. These practices could have potentially exposed personal information, usernames, and passwords. Plaintext, unencrypted communications can be intercepted and read by anyone recording network traffic with free programs like Wireshark.

Defending Against Common Vulnerabilities

First, conduct annual risk assessments based on the quirks of each local system, as systems vary from local government to local government and state to state due to the Help America Vote Act (HAVA) of 2002, which left details on technology and implementation to the states. These assessments may require additional funding and IT support from federal or state governments, as election officials frequently lack funding and IT support. Given the

current lack of cooperation between parties in the U.S. government, this will take actions by individual states or a coordinated effort by citizens across parties to raise the profile of this issue.

Second, upgrade or replace databases and software on a regular basis. Old databases and software like Windows XP or Windows 2000 are no longer supported and vulnerable to attack. Vulnerabilities in these systems are publicly available online via government contractor The MITRE Corporation's CVE website, as well as other sites. Similarly, additional funding and support may be needed from federal or state governments due to lack of funding and IT support.

Third, adopt cybersecurity best practices: limit access, keep backups and logs, and audit activity. In order to prevent identity theft attacks on U.S. voters, adopt user verification methods that don't rely on potentially compromised, commonly used identifiers, such as driver's license numbers and Social Security numbers. Limit the amount of information stored in databases to what's required to register to vote or administer elections, limit access to databases as much as possible, secure workstations, and educate employees about security. Furthermore, keep external backups of registration lists, including paper backups, and audit registrations on a frequent basis to look for abnormal and potentially fraudulent activity. This activity could take the form of high traffic volume or traffic at unexpected times, for example. Finally, record and review logs of all server requests on a regular basis.

Conclusion

In summary, U.S. voter databases are vulnerable to fraud and attack by hackers and even foreign governments. Action needs to be taken to secure voter databases and protect U.S. elections. This needs to be a bipartisan issue. Basic education can eliminate some vulnerabilities. However, others will require more effort to fix. Further securing our systems will require funding and support from government, IT, and cybersecurity professionals. Citizen action is needed to further raise the profile of these issues so we can gain the necessary funding and support from state governments or the federal government.

References

"Checklist for Securing Voter Registration Data." *U.S. Election Assistance Commission.* Accessed December 12, 2017. https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf

Cole, Matthew, Richard Esposito, Sam Biddle, and Ryan Grim. "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election." *The Intercept.* June 5, 2017. https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

"Interstate Crosscheck FOIA Documents." *Indivisible Chicago*. Last updated November 5, 2017. https://www.indivisiblechicago.com/crosscheck-documents/

"Help America Vote Act." *U.S. Election Assistance Commission.* Accessed December 12, 2017. https://www.eac.gov/about/help-america-vote-act/

Calabresi, Massimo. "Inside the Secret Plan to Stop Vladimir Putin's U.S. Election Plot." *Time*. July 20, 2017. http://time.com/4865982/secret-plan-stop-vladimir-putin-election-plot/

Norden, Lawrence and Ian Vandewalker. "Securing Elections From Foreign Interference." *Brennan Center for Justice at New York University School of Law.* June 29, 2017. https://www.brennancenter.org/publication/securing-elections-foreign-interference

"Online Voter Registration." *Pew Charitable Trusts.* May 2015. http://www.pewtrusts.org/~/media/assets/2015/05/ovr_2015_brief.pdf

Sweeney, Latanya, Ji Su Yoo, and Jinyan Zang. "Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections." *Journal of Technology Science.* September 6, 2017. https://techscience.org/a/2017090601/

Vickery, Chris and Dan O'Sullivan. "The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans." *UpGuard.com.* Last updated November 28, 2017. https://www.upguard.com/breaches/cloud-leak-chicago-voters

Vickery, Chris and Dan O'Sullivan. "The RNC Files: Inside the Largest U.S. Voter Data Leak." *UpGuard.com.* Last updated December 11, 2017. https://www.upguard.com/breaches/the-rnc-files

"Securing Voter Registration Data." *United States Computer Emergency Readiness Team*. Last updated September 30, 2016. https://www.us-cert.gov/ncas/tips/ST16-001

"Voting System Security and Reliability Risks." *Brennan Center for Justice at New York University School of Law.* August 30, 2016. https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf