

## Can the Vote Really Be Hacked?

The possibility of voter fraud has made recent headlines, with some arguing it is a widespread problem. While statistics suggest that voting fraud in the US is quite rare, it is not unprecedented, as this article will demonstrate. As we rapidly approach Election Day, it may be worthwhile to examine a variety of traditional voter fraud techniques that hackers could conceivably adapt to today's digital context to undermine the integrity of our voting system.

### BACKGROUND

A 1982 Report of the Special Grand Jury into voter fraud allegations following an election contest between Republican Governor James Thompson and Democratic Party challenger Adlai Stevenson III provides one of most comprehensive overviews of voter fraud in the United States preceding the Internet era.

After results were in, a precinct worker in Chicago claimed to have witnessed voter fraud. The subsequent investigation by the US Attorney and FBI uncovered several methods used by a precinct captain to ensure his precinct would be won by the Democratic Party, including a system for creating false votes which involved the use of early vote-counting computers.

The Grand Jury's report exposed how checks and balances were circumvented and is considered instrumental in the creation of many of the election reforms still in place today.

What is especially interesting to consider is the types of voter fraud outlined in the report, most of which remain possible attack vectors over 30 years later, but which can now be executed on a much broader scale thanks to significant advances in digital technology.

For each of the categories of fraud outlined below, it is easy to imagine a scenario in which a hacker might employ similar methods on a much larger scale in today's digital environment.

### THE ABSENT VOTER

Non-active voters are an ideal target for fraud. They are legal residents, registered to vote, they just choose not to.

In Illinois, the law requires a survey to determine if voters are still alive and living at their registered address. The Grand Jury report outlined how some precinct captains used the Illinois-mandated canvas survey to compile "eligible voter" lists showing which legitimate voters would not be available for the vote. In some instances, canvassers would ask potential voters whether they were likely to vote and even survey boarding houses to establish who was too sick, too drunk or otherwise not able to vote. The precinct captain or delegated representative would then "vote" for the people who hadn't or couldn't vote.

In today's world, it is arguably easier to access this kind of voter information. In June 2016, Chris Vickery, a security researcher at the cybersecurity firm MacKeeper, uncovered a database with the voter registration records of 191 million voters which had been exposed online. Voter reg-

istration lists include name, address, political party, telephone number, and whether the voter voted in the last elections and primaries. Subsequently, the FBI reported that state voter lists were hacked in Arizona and Illinois.

For fraudsters today, it is easy to corroborate this data via apps and social media activity. Even perfectly legitimate banner-ad-based or email-based web surveys could be used to flesh out information.

A hacker able to access tabulated vote records would make this data even more actionable. For example, knowing the past history of a voter's behavior would allow a hacker to pick absentee voters who are likely to "vote" a certain way with minimal risk of signaling an unusual pattern – for example, someone who votes Democratic 100% in the past who suddenly voted Republican in a new election would be unusual. The list of non-participating voters could be monetized, either through in-person false representation or, more efficiently, by a direct feed of "votes" into the tabulation system.

This type of fraud would be difficult to detect without the presence of a similar correlation effort like intensive analysis of a voter's past behavior or via a direct survey of voters. From a risk mitigation standpoint, big data analysis of voting patterns could uncover unusual last-minute voting activity compared to past votes, but ultimately direct and expensive investigation would be necessary to identify fraud of this kind.

#### **FALSE REGISTRATION**

The Grand Jury report cited several instances whereby individuals were offered incentives to register falsely in person. A similar strategy could be effective today.

As of June 2016, a total of 31 states plus the District of Columbia offer online registration, and another seven states have passed legislation to create online voter registration systems. Online voter registration may provide new ways for individuals to register under another person's name. A cross-comparison between existing voter databases and census databases, for example, could easily provide hackers with a pool of potential voters who are currently unregistered. Validation methods to establish voter eligibility for registration will need to maintain consistently high standards to avoid potential manipulation as online registration becomes the norm. At a minimum, basic e-commerce validation should be performed to ensure, for example, that multiple registrations do not occur from the same IP address.

#### **FRAUDULENT USE OF ABSENTEE BALLOTS**

The Grand Jury report detailed how some voters in Illinois were encouraged to apply for absentee ballots, even though they planned on voting in person. After comparing lists of eligible voters against actual vote lists, the blank absentee ballots were used to add fraudulent votes.

The ability to request absentee ballots online dramatically increases the potential scale of fraud in this scenario and, combined with information available online via hacked voter databases, increases the ease of implementation.



## VOTE BUYING

The Grand Jury report noted drunks and transients were paid to vote. A hacker equivalent could take many forms: Bitcoin payments in the dark web or perhaps the creation of “paying gigs” through on-demand workforce services such as Amazon Mechanical Turk, TaskRabbit and Gig-walk. The idea is that registering and voting for a specific candidate could become a “gig economy” task.

## ALTERING THE VOTE COUNT

According to the report, one precinct captain ran a single Democratic punch card 198 times through the voting machine, followed by six punches of a Republican card. This is possibly one of the earliest examples of computer-related voting fraud.

In modern times, of course, the enterprising hacker would test all avenues of the voting system. Could the voting machines be accessed? Could the voting machines’ channel to the central tabulating server be accessed? Could the server itself be accessed? Could voter ID or other voting requirements be spoofed? The attack methods would depend on the avenue deemed easiest to access: malware for the voting machines, either custom-installed or via tampered firmware updates; man-in-the-middle or distributed denial-of-service (DDoS) attacks to spoof voting data or prevent it from being communicated; server attacks to alter databases or counting algorithms; attacks to modify voter registration guidelines encoded into online voter registration web sites; attacks to obtain access to up-to-date voter registration data in “get out the vote” canvassing campaigns conducted by legitimate political organizations. The list goes on.

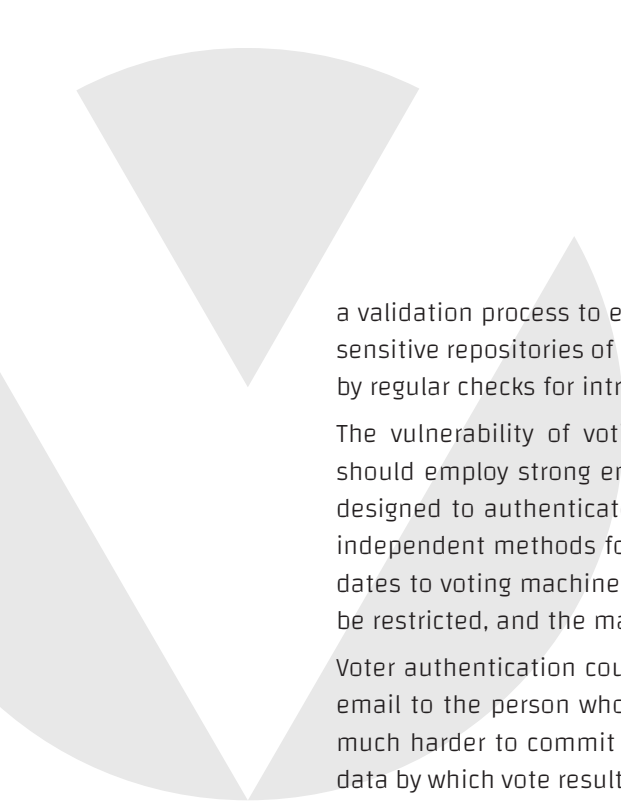
## THE SOLUTION

Hackers could influence the results of an election by any of these means. It is clear the greatest threat for voter fraud doesn’t lie in the potential for tampering with voting machines. While tampering is still possible, to do so without leaving a trace is difficult. The greatest threat to the integrity of the vote is simply the scale which the Internet and other digital tools and techniques make possible.

Consider the potential scalability of false voting registration. Access to voting databases and detailed voter behavior from social media creates the potential for millions of otherwise undetectable fraudulent votes, a process made easier by low voter turnout. If valid voter turnout is 90%, only 10% of the entire population is potentially eligible for fraud, and the impact of fraudulent votes would be relatively low. With less than 50% turnout, however, there is a much higher proportion of potentially fraudulent votes – enough to alter the legitimate outcome.

Fortunately, there are tools and processes which can tackle this kind of cybercrime and keep elections honest.

In cybersecurity, fraudulent representation is combatted via authentication, which ensures that a person or computer process is who they say they are, that any transfer of information includes



a validation process to ensure that source and destination are who they say they are, and that sensitive repositories of information and critical systems are protected by restricted access and by regular checks for intrusion.

The vulnerability of voting machines has already been well-documented. Voting machines should employ strong encryption and authentication to servers collecting data. They must be designed to authenticate that data submitted is from a valid voter, and there should also be independent methods for voters to check that their vote was tabulated correctly. Firmware updates to voting machines should be code-signed. Physical access to voting machines needs to be restricted, and the machines themselves should employ anti-tampering technology.

Voter authentication could be conducted by sending an SMS confirmation of a vote and/or an email to the person who supposedly voted. This “two-factor” authentication method makes it much harder to commit voter fraud of any kind – not least by creating an independent set of data by which vote results can be validated against and by bringing additional sources of review to the process.

Transparency and outside expert validation should also be considered. Experts in digital forensics – whether public or private – are well-equipped to examine all levels of the voting process to detect fraud. There is also the opportunity to leverage machine learning and big data analyses of present and past voting patterns to identify anomalies and potential improper activity.

## CONCLUSION

We can never be complacent about hackers, particularly when it comes to elections and democracy. While the methods of voter fraud have not substantially changed, the scale at which these methods can be deployed has. The tools exist to combat the potential for hackers to commit voter fraud; it is imperative that they are put in place.