Voting vulnerability: Study points to potential fraud in online voting registration systems

September 6 2017

Credit: Karen Arnold/public domain

Online attackers may be able to purchase - for as little as a few thousand dollars - enough personal information to potentially alter voter registration information in as many as 35 states and the District of

Columbia, according to a new Harvard study.

Dubbed "voter identity theft" by study authors Latanya Sweeney, Professor of Government and Technology in Residence, research analyst Ji Su Yoo and graduate student Jinyan Zang, the vulnerability could be exploited by attackers to attempt to disenfranchise many voters where voter registration information can be changed online. Armed with personal information obtained through legitimate or illegitimate sources, hackers could know enough to impersonate voters and change key information using online voter registration systems.

One tactic, researchers said, would be to simply change voters' addresses, making it appear - to poll workers at least - as though they were voting at the wrong location. Those voters might be forced to cast provisional ballots, which in many circumstances are not counted. The study is described in a September 6 paper published in the *Journal of Technology Science*.

Though the researchers don't report evidence of attackers exploiting the vulnerability, Sweeney, Yoo and Zang said the fear is that it might be used to either undermine confidence in elections or even to swing the result in favor of a particular candidate.

"If the goal is to undermine any belief in the electoral system, then they might very well want to target a particular community at large...(because) that could cause a kind of hysteria," Sweeney said. "People will say what kind of system is this? We didn't get a chance to vote, our whole community didn't get a chance to vote."

"If you look at the outcome of the 2016 election...there were several states where the margin of victory was within one or two or five percent," she continued. "If you want to change the result in a state that was determined by less than one percent of the votes, what is the

smallest number of changes you can make and where do you make them?"

In the hope of preventing attackers from exploiting the vulnerability, Sweeney, Yoo and Zang notified election officials from the vulnerable states of their findings prior to publication, attended a national convention of such officials to discuss the findings, and will hold a workshop, to which election officials have been invited.

"Most states do have back office processes and election practices that could detect or limit an attack, but there is room for improvement," Sweeney said.

Obtaining the information needed to make those changes, Sweeney said, is far easier than most would believe, because contrary to popular opinion, voter information isn't private.

Data sets containing voter names and demographic information like addresses, party affiliation and even gender can be purchased or downloaded - often from government sites themselves - for only a few dollars. For just $18,000, researchers were able to buy voter lists from all 35 states, and Washington, D.C., that allow online registration.

Those lists, however, don't contain the personal information - like Social Security or driver's license numbers - most states use to confirm a voter's identity online. Finding that, Sweeney said, was as simple as forking over $40 per month for access to a commercial data broker site.

"The law says only people in certain situations are able to buy this data - one choice is if you want to search for your own data or for fraud investigations - but it's based on a self-attestment," Sweeney said. "That gives the brokers coverage, so if the government says you shouldn't have sold the data to that person, they can say it's not our fault, they said they

were using it for this purpose."

While it is possible to find the information needed to alter voter information through legal means, Sweeney said the dark Web offered one major advantage - cost.

For just $1,002, an attacker could purchase two datasets - one believed to have come from a massive data breach of credit bureau Experian - that contained the names, address, dates of birth, gender, and Social Security numbers of most adult Americans.

Armed with that information, Sweeney, Yoo and Zang said, attackers could theoretically access and alter the voting information of thousands of individuals. In some states, they found, it would cost a mere $1 to change one percent of voter records, while the median cost was just $41.

"The money, I think that's a real shocker," Sweeney said. "When we first talked about this project with a Washington insider, he told us we were wasting our time, because voter data is so expensive. His prediction was that we would only succeed on a few sites...and that was because he thought the only way to get the data was from the state.

"But it turns out you can get it from many states, and only a handful charge a per-voter cost, which dramatically increases the cost," she added. "In Ohio, the data is free - you can download it from the Web. And others who have purchased the data have made it freely available in an attempt to add transparency to the election process. Even data brokers who specialize in voter lists, $2,000 was the maximum, and they covered all 50 states."

Sweeney conceded, however, that altering voter information may not be as simple as finding the right data.

Although it may be relatively easy to gain access to the Social Security and driver's license numbers needed to make changes to voter information, Sweeney said states may have additional security - such as having officials review and confirm address changes - that could halt an attack before major damage is done.

While those efforts may have so far been successful, Sweeney, Yoo and Zang, are urging states to take additional steps to protect against potential attacks. "A human may notice if a larger than usual number of changes appear, but what if the number is only a few more a day? A computer program might do better." said Sweeney.

"Our paper is not trying to be critical of the government or suggest that the government didn't invest enough money or resources into security," Yoo said. "But it's just the nature of government that it moves at a different pace than commercial technology does."

Among the key steps researchers urge states to take, if they are not already doing so, is the logging of all site visitors, which could allow officials to track whether a single visitor is responsible for multiple voter information changes, and to track where a potential attack came from.

"We also recommend states keep logs of the changes that are made," Sweeney added. "That would enable them to roll back through the changes, and see what changes were made and how they were changed. Some states have been doing this. We recommend all states do so."

Ultimately, the question the study asks is how can the government ensure it's actually dealing with citizens when it conducts business online. That question is important, Sweeney said, because although commercial fraud is a problem, the stakes are far higher for the government.

"If a commercial site is compromised, the downsides are not the same,

because it doesn't compromise our entire democratic process," Sweeney said. "When people talk about voter fraud, what they usually mean is additional votes being cast by one party, but this is different. It's about people who should have been able to vote, but can't. This fits into the larger discourse of election security in a unique way...because it could allow for a particular group to be disenfranchised."

Provided by Harvard University