Researchers identify security vulnerabilities in voting app

February 13 2020, by Abby Abazorius

Credit: Massachusetts Institute of Technology

In recent years, there has been a growing interest in using internet and mobile technology to increase access to the voting process. At the same time, computer security experts caution that paper ballots are the only

secure means of voting.

Now, MIT researchers are raising another concern: They say they have uncovered security vulnerabilities in a mobile voting application that was used during the 2018 midterm elections in West Virginia. Their security analysis of the application, called Voatz, pinpoints a number of weaknesses, including the opportunity for hackers to alter, stop, or expose how an individual user has voted. Additionally, the researchers found that Voatz's use of a third-party vendor for voter identification and verification poses potential privacy issues for users.

The findings are described in a new technical paper by Michael Specter, a graduate student in MIT's Department of Electrical Engineering and Computer Science (EECS) and a member of MIT's Internet Policy Research Initiative, and James Koppel, also a graduate student in EECS. The research was conducted under the guidance of Daniel Weitzner, a principal research scientist at MIT's Computer Science and Artificial Intelligence Lab (CSAIL) and founding director of the Internet Policy Research Initiative.

After uncovering these security vulnerabilities, the researchers disclosed their findings to the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). The researchers, along with the Boston University/MIT Technology Law Clinic, worked in close coordination with election security officials within CISA to ensure that impacted elections officials and the vendor were aware of the findings before the research was made public. This included preparing written summaries of the findings with proof-of-concept code, and direct discussions with affected elections officials on calls arranged by CISA.

In addition to its use in the 2018 West Virginia elections, the app was deployed in elections in Denver, Oregon, and Utah, as well as at the 2016 Massachusetts Democratic Convention and the 2016 Utah

Republican Convention. Voatz was not used during the 2020 Iowa caucuses.

The findings underscore the need for transparency in the design of voting systems, according to the researchers.

"We all have an interest in increasing access to the ballot, but in order to maintain trust in our elections system, we must assure that voting systems meet the high technical and operation security standards before they are put in the field," says Weitzner. "We cannot experiment on our democracy."

"The consensus of security experts is that running a secure election over the internet is not possible today," adds Koppel. "The reasoning is that weaknesses anywhere in a large chain can give an adversary undue influence over an election, and today's software is shaky enough that the existence of unknown exploitable flaws is too great a risk to take."

Breaking down the results

The researchers were initially inspired to perform a security analysis of Voatz based on Specter's research with Ronald Rivest, Institute Professor at MIT; Neha Narula, director of the MIT Digital Currency Initiative; and Sunoo Park SM '15, Ph.D. '18 , exploring the feasibility of using blockchain systems in elections. According to the researchers, Voatz claims to use a permissioned blockchain to ensure security, but has not released any source code or public documentation for how their system operates.

Specter, who co-teaches an MIT Independent Activities Period course founded by Koppel that is focused on reverse engineering software, broached the idea of reverse engineering Voatz's application, in an effort to better understand how its system worked. To ensure that they did not

interfere with any ongoing elections or expose user records, Specter and Koppel reverse-engineered the application and then created a model of Voatz's server.

They found that an adversary with remote access to the device can alter or discover a user's vote, and that the server, if hacked, could easily change those votes. "It does not appear that the app's protocol attempts to verify [genuine votes] with the back-end blockchain," Specter explains.

"Perhaps most alarmingly, we found that a passive network adversary, like your internet service provider, or someone nearby you if you're on unencrypted Wi-Fi, could detect which way you voted in some configurations of the election. Worse, more aggressive attackers could potentially detect which way you're going to vote and then stop the connection based on that alone."

In addition to detecting vulnerabilities with Voatz's voting process, Specter and Koppel found that the app poses privacy issues for users. As the app uses an external vendor for voter ID verification, a third party could potentially access a voter's photo, driver's license data, or other forms of identification, if that vendor's platform isn't also secure.

"Though Voatz's privacy policy does talk about sending some information to third parties, as far as we can tell the fact that any third party is getting the voter's driver's license and selfie isn't explicitly mentioned," Specter notes.

Calls for increased openness

Specter and Koppel say that their findings point to the need for openness when it comes to election administration, in order to ensure the integrity of the election process. Currently, they note, the election process in

states that use paper ballots is designed to be transparent, and citizens and political party representatives are given opportunities to observe the voting process.

In contrast, Koppel notes, "Voatz's app and infrastructure were completely closed-source; we were only able to get access to the app itself.

"I think this type of analysis is extremely important. Right now, there's a drive to make voting more accessible, by using internet and mobile-based voting systems. The problem here is that sometimes those systems aren't made by people who have expertise in keeping voting systems secure, and they're deployed before they can get proper review," says Matthew Green, an associate professor at the Johns Hopkins Information Security Institute. In the case of Voatz, he adds, "It looks like there were many good intentions here, but the result lacks key features that would protect a voter and protect the integrity of elections."

Going forward, the researchers caution that software developers should prove their systems are as secure as paper ballots.

"The biggest issue is transparency," says Specter. "When you have part of the election that is opaque, that is not viewable, that is not public, that has some sort of proprietary component, that part of the system is inherently suspect and needs to be put under a lot of scrutiny."

More information: The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections: internetpolicy.mit.edu/wp-cont … isOfVoatz_Public.pdf

This story is republished courtesy of MIT News

(web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology