Internet Voting Deserves Second Look, Say Researchers

LOS ANGELES, CA / October 28, 2020 / Internet voting, lacking voter privacy and auditability, along with a litany of other intractable security problems, is something many people think should never come, but a prominent international team of cryptographers and election security experts are calling for a second look. The team, led by Dr. David Chaum—widely recognized as the father of digital currency—says their project, *VoteXX*, imagines a world that brings the promised convenience of online banking to your voting experience.

While it is seen as the "holy grail" of voter experiences, Internet voting is also widely seen as dangerous to election integrity. This position has near universal agreement from the research community, and even some members of the team are on record opposing it. But, there is a relentless, global push to vote online that continues to grow louder.

For years, we have heard the most prominent cybersecurity experts tell us how insecure online voting systems are, recently with Voatz[1] and Scytl,[2] but there is no such thing as a "secure" Internet voting system, despite the claims made by vendors. Renowned MIT cryptographer Ronald Rivest is unequivocal on this point, admonishing in 2010, "Best practices for Internet voting are like best practices for drunk driving."[3]

"Nearly every vendor characterizes their products as being completely secure, but that statement has never been true, will never be true, and is not good enough." says Dr. Richard Carback, a member of the VoteXX team. "In Internet voting, the design must assume every component is or will be compromised." The task seems impossible.

[1] `https://cointelegraph.com/news/voatz-blockchain-app-used-in-us-elections-has-numerous-security-issues-says-report`

[2] `https://www.computerworld.com/article/3471519/flaw-in-nsw-s-ivote-platform-confirmed-by-researcher.html`

[3] `https://people.csail.mit.edu/rivest/pubs/Kan10.pdf`

Elections require public trust; there is only one chance to get it right; and the stakes are enormous. It is not enough to declare a winner—the system must also convince the losers that they lost. The key is that voters must be able to verify that their ballots were received and that all votes were counted accurately, as they were cast. At the same time, voters should not be able to sell their vote or be coerced, which is a difficult task in the age of ubiquitous recording devices.

Even the most advanced computing devices and methods today cannot provide these assurances. Voting by mail today offers no protection against a voter filling out the ballot under the watchful eyes or from the receiving end of a streaming phone of a coercer or vote buyer. Uploading your vote to an indelible blockchain means nothing if your computer changes it to the wrong vote, or your Internet is down for the entire voting period. Furthermore, the system must not spy on how you voted.

To deal with these issues, VoteXX offers a mix of simple strategies and complex cryptography. The strongest technique in VoteXX is how it mitigates vote selling. Given that a voter can record the entire process of receiving and casting their ballot, how could the system stop someone determined to sell their vote? "Simple," says David, "You make it possible to flip (change or cancel) that vote outside the voting process. Because a vote buyer cannot be sure you didn't or won't flip your vote, they can't be sure that a voter has been honest with them, making it useless to buy votes."

This "*vote flipping*" approach provides a subversively simple yet powerful tool to voters. It's accomplished by creating a "*flip code*" during the registration process that allows the voter to flip their vote after casting. Proof of knowledge of the flip code can be shared to any third parties, which the team playfully dubs *hedgehogs*, who can then post the proof anonymously to flip a vote.

To handle network outages, power outages, and other connectivity issues that could plague an Internet election, VoteXX assumes long periods of time to vote. "The idea is not unlike what we already see in vote-by-mail, where election officials send out ballots with as much time as possible to avoid issues with mail delays and inclement weather," says Alan Sherman, professor of computer science at UMBC. "It's expensive to pay for a continuous denial-of-service attack over a long period of time, and a longer voting period also provides ample time for election officials and voters to respond to and mitigate the threats."

To thwart malware and prove to voters that their ballots are cast, col-

lected, and counted properly, the system uses a "remote code voting" technique, which they pioneered at Takoma Park in 2011, to elect the mayor and city council. Their system is called *Remotegrity*. In it, voters received scratch-off cards with secret codes used to vote for their candidates. These codes hide voter choices from the computers they use and from the only on-line component of the system, which simply collects vote codes.

The researchers stress that the underlying strategy to protect the integrity of the system is simple: make every computer involved commit to what it will do in a digital audit trail, by printing or posting, without revealing how people voted. Voters and auditors then audit everything end-to-end, confirming accuracy of the results. This strategy turns the malware problem on its head, making it necessary for malware to control every computer that will ever access the data, instead of requiring election officials and voters to make sure that their computers are free from malware.

These techniques, or versions of them, can be used to create safe and secure Internet election systems. "Remote voting is already here—it's called vote-by-mail, and the absence of vote-selling protection is extremely concerning to me," says David. "We have a long history in this country of people selling their votes. It's high time for a national effort to make remote voting, whether through the Internet or by mail, as secure as we can make it."

Notably, the researchers aren't simply hawking their system as vendors do, but instead are calling for national support of serious research and development for Internet voting. Given the vital importance of voting technologies, Sherman is leading the team's effort to urge Congress to create a nonpartisan National Research Center for the Technologies of Democracy. Such a center could study a wide range of issues pertaining to elections including voting systems, reporting systems, ballot design, usability and accessibility, election methods (e.g., plurality, range voting, instant runoff), and how to define voting districts. Such a center could be created as part of the existing well-funded National Cybersecurity FFRDC.

Members of the team include David Chaum, Richard Carback, and Mario Yaksetig (xxnetwork, Los Angeles, CA, USA), Jeremy Clark and Mahdi Nejadgholi (Concordia University, Canada), Alan T. Sherman and Chao Liu (UMBC, MD, USA), Filip Zagórski (Wroclaw University of Science and Technology, Poland), and Bart Preneel (Katholieke Universiteit, Leuven, Belgium).

To learn more, see `https://votexx.org`

Contacts: David Chaum, info@chaum.com; Richard Carback, rick@xx.network; Alan T. Sherman, sherman@umbc.edu