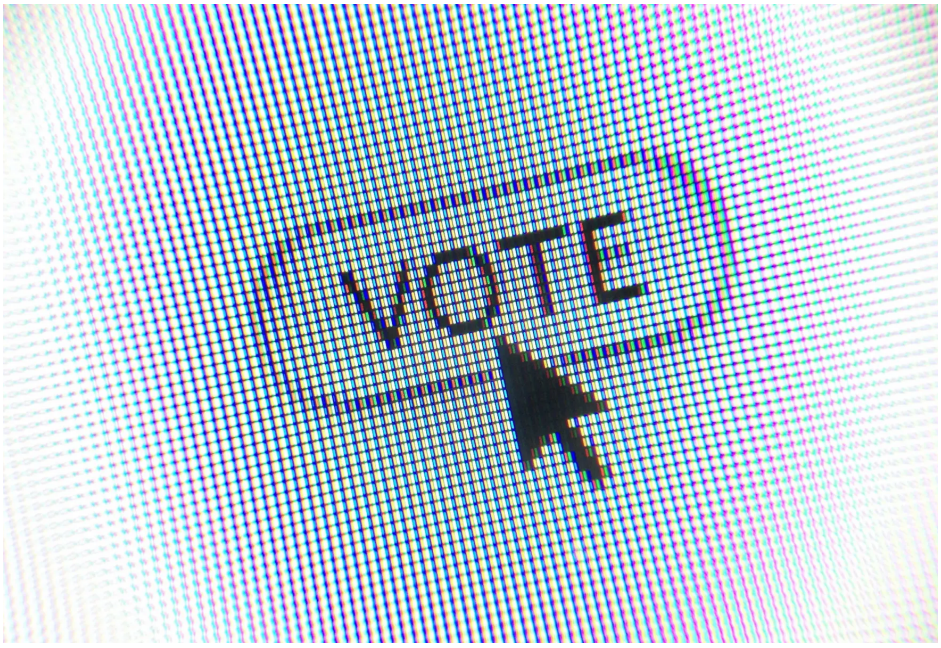


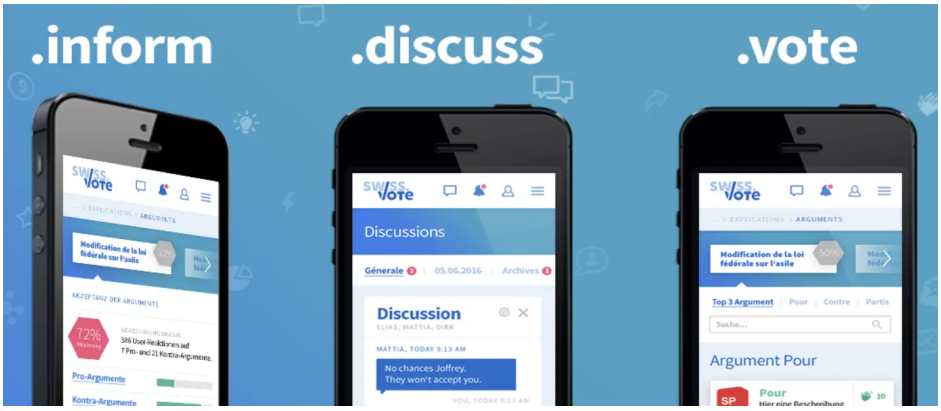
WHAT A SECOND FLAW IN SWITZERLAND'S SVOTE MEANS FOR NSW'S IVOTE

A recent investigation found a trapdoor in the SwissVote election system that also exists in New South Wales' iVote, but further analysis has found a second problem in the verification process

By Associate Professor Vanessa Teague, University of Melbourne

Earlier this month, research by our team (https://about.unimelb.edu.au/newsroom/news/2019/march/researchers-find-trapdoor-in-swissvote-election-system) – based on joint work with Sarah Jamie Lewis from the Open Privacy Research Society and Professor Olivier Pereira at Université Catholique de Louvain – found a trapdoor in the Swiss Internet voting system. It's a flaw in the proof (https://people.eng.unimelb.edu.au/vjteague/SwissVote.html) the system uses to prevent electoral fraud.

The sVote Internet voting system is designed to allow observers to verify that the votes reported by the electoral commission match those that were cast — without compromising the identity of a voter. But if the flaw is exploited, it could allow insiders who ran or implemented the election system to modify votes undetected.



The researchers found a trapdoor in SwissVote election system. Picture: SwissVote

Soon after the Swiss trapdoor was revealed, the New South Wales Electoral Commission (NSWEC) announced that the same flaw affects their iVote system (https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post-e-vo) . The two systems, the Swiss and the NSW e-voting software, were developed by the same company and feature the same core component.

But the Commission has since said that its iVote platform is safe (https://www.sbs.com.au/news/serious-flaw-hits-nsw-voting-system) to use in the state's recent election.

However, we have recently discovered a second, independent method by which a proof mechanism in sVote could be subverted to *prove* an election outcome that has actually been manipulated.

SwissPost and NSWEC have both been notified, and NSWEC says that this second issue does not affect them (https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Media%20Release/190322-NSW-Electoral-Commission-iVote-and-Swiss-Post-e-voting-update.pdf)

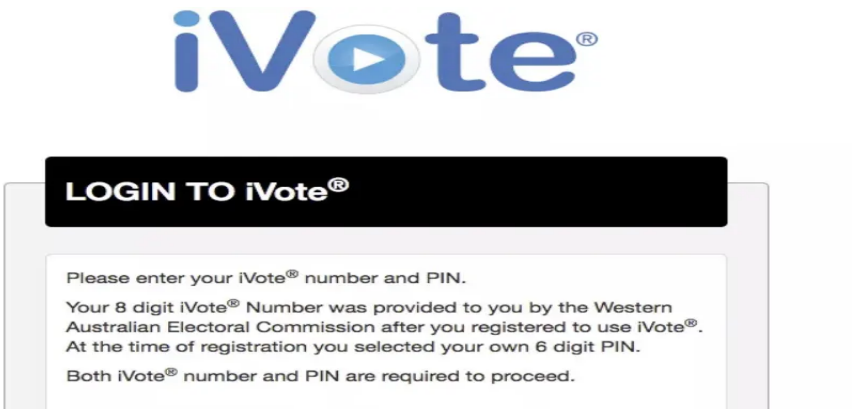
.

VERIFIABILITY AND TRUST

Verifiability is a critical part of the trustworthiness of e-voting systems.

The SwissPost e-voting system, (https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting) provided by Scytl, offers one form of verifiability, called "complete verifiability" – this means that any manipulation should be detectable unless all but one part of the system colludes to cheat.

In the SwissPost system, encrypted electronic votes are shuffled to protect individual vote privacy. Each server shuffling votes is supposed to prove that the set of input votes it gets correspond exactly to the differently-encrypted votes it outputs.



The New South Wales Electoral Commission says this second issue doesn't affect them. Picture: iVote

This process is intended to provide an electronic version of a ballot box.

Previously, we've shown that this system contains a cryptographic trapdoor (https://people.eng.unimelb.edu.au/vjteague/SwissVote.html) that could allow a cheating authority (or software provider) to add or remove votes from the shuffle, while providing an apparently-correct (but false) proof of accuracy.

Both SwissPost and NSWEC say that the software provider has now patched the issue.

PROVING A FAKE DECRYPTION

The next step after shuffling is decrypting the votes.

It wouldn't be secure to simply accept any authority's claim of what those encrypted votes contain, because that allows for the possibility that the authority could declare different votes from the voter's actual choice.

It also wouldn't work to ask the authority to reveal its private decryption key, because that would expose how individuals voted.

So, the sVote system uses a clever cryptographic construct called a *zero knowledge proof*. Zero knowledge means that it doesn't reveal anything about the decryption key, so vote privacy is protected. And proof is supposed to mean that observers can run a verification algorithm to make sure that the claimed vote really is what's hidden within the encryption.

But our research (https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf) has found that this proof is not sound. It's possible to generate a proof that passes verification, but changes the contents of the encrypted vote. It's a little like leaving the ballot box observable all through polling day, yet somehow managing to slip different votes into the count.

Verifiability is a critical part of the trustworthiness of e-voting systems. Picture: Getty Images

It's a technical process – but one that can be done by anyone who has access to the right part of the voting system. You can download our cheating proof transcripts (https://people.eng.unimelb.edu.au/vjteague/SwissVoteDecryptionCheat.zip) and verify them yourself if you have the sVote code.

INTERNET VOTING SECURITY

Both SwissPost and NSWEC say they have corrected the first issue – the shuffling proofs. Of course, without seeing the patched source code we have to take their word for it.

But the second issue, the unsound decryption proofs, was only noticed very recently and as far as we're aware it has yet to be corrected. NSWEC says their decryption proofs are not affected, but without seeing the source code this can't be checked.

So, what does this mean for Internet voting security?

First of all, it means that Australians should be grateful to Switzerland for passing a Federal Ordinance mandating open access to the source code (https://www.admin.ch/opc/en/classified-compilation/20132343/index.html#a7b) of their voting system.

Open, public review is important even for systems that are intended to be verifiable, because the voters and candidates need to be convinced that it will not seem to verify something that is wrong. Otherwise, the risk of undetectable electoral fraud remains, because of the risk that the verification mechanism itself might be manipulated.

The second flaw is like ballot box observable all through polling day, yet somehow managing to slip in different votes. Picture: Getty Images

It's lucky that a problem in iVote could be discovered by inspecting the Swiss code, because the iVote code is available only under very restrictive terms that would not have allowed us to analyse the code and publish our findings promptly.

Were it not for the opportunity to examine the Swiss Post code, opportunities for undetectable electoral fraud might have gone unnoticed in the NSW election.

THE BOTTOM LINE

We have now found two, independent means by which a single authority could commit large-scale fraud in the sVote system, while passing verification using a false proof that everything was correct.

For iVote, we're told that the first issue has been patched and the second doesn't apply. If the source code were openly available, we could check; without it, we can't.

There's no reason to think that correcting this second flaw in the proofs will be easy, or that it will produce a secure system with no further opportunities for undetectable electoral fraud.

Banner: Getty Images

First published on 25 March 2019 in **Engineering & Technology**

ENCRYPTION | INTERNET SECURITY | CYBERSECURITY | ELECTIONS | ELECTRONIC VOTING

Featured


Associate Professor Vanessa Teague
Chair, Cybersecurity and Democracy Network, School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne


Sarah Jamie Lewis
Executive Director, Open Privacy Research Society


Professor Olivier Pereira
UCL Crypto Group, Université Catholique de Louvain

Recommended for you

ENGINEERING & TECHNOLOGY

iVote West Australia: Who voted for you?

Voters casting their ballot online must be able to trust the process. In a world where hackers have been accused of interfering in elections, iVote is not the answer