Researchers find trapdoor in SwissVote election system

12 March 2019

In the SwissPost system, encrypted electronic votes need to be ‘shuffled’ to protect individual vote privacy. Credit: Pixabay

A team of researchers have examined the source code published as part of the SwissPost e-voting system, provided by Scytl, and discovered a cryptographic trapdoor.

If exploited, researchers say this could allow insiders who ran or implemented the election system to modify votes undetected.

University of Melbourne Vanessa Teague from the School of Computing and Information System conducted the research with Sarah Jamie Lewis from Open Privacy Research Society (Canada) and Olivier Pereria from Université Catholique de Louvain (Belgium).

In the SwissPost system, encrypted electronic votes need to be 'shuffled' to protect individual vote privacy.

The authority who conducts the shuffle is supposed to provide a mathematical proof that no votes have been changed. This allows the election result to be verified.

But the trapdoor found in this code allows an authority to produce a proof that seems to verify correctly actually alters votes.

"The existence of a trapdoor is worrying," Ms Lewis said.

"While nothing in our analysis suggests that this problem was introduced deliberately, its mere presence raises serious questions about the rest of the code."

This isn't the first time that researchers have identified serious flaws in internet voting systems.

Analysis of other systems in Washington DC, Estonia, New South Wales and Western Australia have raised serious concerns about privacy, integrity and verifiability.

"In this case, our analysis of the code shows errors that are consistent with a naïve implementation of a complex cryptographic protocol by well-intentioned people who lacked a full understanding of its security assumptions," Associate Professor Teague said.

"Of course, if someone did want to introduce an opportunity for manipulation, the best method would be one that could be explained away as an accident if it was found. We simply do not see any evidence either way."

Researchers have shared the finding with SwissPost, who say they have now addressed the problem.

Ms Lewis, Professor Pereira and Associate Professor Teague have also published a paper that explains the technical details of the trapdoor and how an insider could exploit it to undetectably alter election results.

More information: Trapdoor commitments in the

SwissPost e-voting shuffle proof.
people.eng.unimelb.edu.au/vjteague/SwissVote

Provided by University of Melbourne