Vicky the Viking and universal verification

12.02.2019

Prof. Dr. Rolf Haenni and Prof. Dr. Reto E. Koenig, Bern University of Applied Sciences, Research Institute for Security in the Information Society, https://e-voting.bfh.ch.

Security Cantons

Vicky the Viking lives in the village of Flake. Time after time, he succeeds in defending his village against powerful attackers thanks to his many clever ideas. Similarly, many clever ideas have been developed in research to protect e-voting against powerful attackers. The most important of these is universal verification. A guest column from Prof. Dr. Rolf Haenni and Prof. Dr. Reto E. Koenig.

Whenever Runer Jonsson's stories about "Vicky the Viking" mention that Sven the Terrible's ship is on the horizon, there seems to be no way out for the inhabitants of the Viking village of Flake. Sven the Terrible is too big and strong, his intentions too evil and sneaky, the spikes of his flail too pointed and sharp and the warriors on his ship too numerous and determined. The fate of Flake seems sealed.

In every hopeless situation, however, the clever Viking boy Vicky succeeds in saving his village from Sven the Terrible with a brilliant idea. The leader of Flake, Vicky's father Halvar, is very sceptical, but he has no choice but to help implement Vicky's plan. Halvar only gradually notices that this is actually working, when Sven's attacks are ineffective and he finally has to return home. Because Vicky's ideas are original and surprising, the attackers encounter a defence strategy that their weapons cannot counteract.

The same is true of e-voting in Switzerland, when powerful countries such as Russia, China or the USA have an interest in a particular outcome of a federal vote. These countries are too big and too strong, their intentions too evil and malicious, their technologies too powerful and too advanced and the hackers who are hired by these countries too numerous and too sophisticated. The fate of democracy in Switzerland seems sealed.

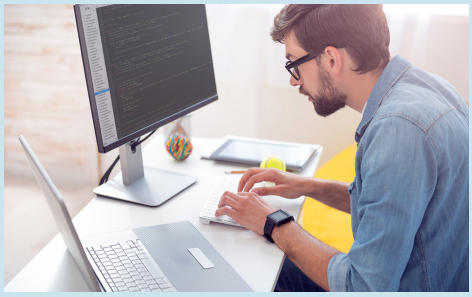
It's a very interesting scientific question, which requires closer examination. Without stopping to consider the issue in depth, critics tend to react prematurely and answer the question with "no". Just like Halvar, Snorre and Faxe, who are initially very sceptical about Vicky's ideas because they cannot understand his lateral thinking. But at least they do not reject Vicky's ideas from the beginning.

Probably the most important idea that has emerged from e-voting research is that of universal verification (also called universal verifiability). Its aim is to provide the electorate with a means of independently verifying the election result. The methods used are designed in such a way that all conceivable manipulation attempts are revealed during verification at the latest. The cryptographic methods used guarantee this with mathematical precision.

There is something similar in traditional elections and votes on paper. If there are doubts about the result of the election, for example if the result is very close, a recount can be requested. Since there are always minor discrepancies in the manual counting of ballots, the result of the recount will never be exactly the same, but in most cases it will suffice to confirm the winners of the election.

Universal verification of electronic voting goes one step further. The cryptographically protected data which is aggregated in the preparation, execution and counting of a vote in a distributed system serves as input for universal verification. In this case, a recount is performed, so to speak, whereby every little discrepancy in the data is revealed during the verification. This mechanism makes it impossible for manipulations to go undetected. In turn, successful universal verification eliminates any doubt about the correctness of the count. There are no minor discrepancies such as with counting paper ballots.

The discussion about the security of e-voting has recently been shaped by those who reject the introduction of e-voting in Switzerland on the basis of fundamental convictions. In most cases, their reasoning is relatively thin, because it essentially consists of exactly the attack scenarios that have driven e-voting research for 30 years. However, the critics do not seem to be really familiar with the results of this research.



Public hacker test on Swiss Post's e-voting system

07.02.2019 | Swiss Post will be carrying out resilience testing, also known as a public intrusion test (PIT), on its e-voting system between 25 February and 24 March 2019. How does the intrusion test work and what happens if anything is found? The answers to the key questions.

More

Swiss Post publishes the source code for its e-voting system

07.02.2019 | Swiss Post is publishing the source code for its e-voting system in accordance with the requirements of the Confederation and cantons. The information published particularly relates to the core elements of the encryption components.

More

Democracy is being entrusted to a company – and other misunderstan

04.02.2019 | Swiss Post welcomes th in-depth reporting and public deba voting, and wishes to share its pers by addressing some recurring misunderstandings.

More