Swiss Post's voting system put through its paces by hackers

Oliver Flüeler (https://post-medien.ch/en/author/flueelero/) 7. February 2019 14:40

Last modified: 7. February 2019 15:19

Swiss Post will be subjecting its e-voting system to a public hacker test from 25 February to 24 March 2019. This will fulfil the directives issued by the Swiss Confederation and cantons. The test – known as an intrusion test – will allow registered IT specialists to put the system through its paces by attempting to manipulate the result of a fictitious ballot contest. Swiss Post will incorporate the results of the hacker test into the development of its e-voting system. Swiss Post publishes today the source code to its system, which independent experts can scrutinize to prepare thoroughly for the intrusion test. This rare approach is not causing any sleepless nights for Denis Morel, Head of E-voting at Swiss Post, as he reveals in our interview. But he is always curious about the creativity and sophistication of highly specialized hackers.

Denis Morel, the Swiss Confederation and cantons have made it a requirement that a public hacker test be performed before a latest generation e-voting system can be used in Switzerland. Is this causing you any sleepless nights?
No, I'm sleeping very well, all things considered. And with good reason: the Swiss Post e-voting system has been in operation for a

number of years, and hackers haven't been waiting for us to announce a specific date for a public stress test on the system. We perform these sorts of intrusion tests in-house every two months or so, in conjunction with specialists from a wide variety of units.

You have already launched an international appeal to find experts to register for the security test in February. Will Swiss Post be inundated with applications?

Interest in the test is indeed very high. We have received 450 advance applications. Public hacker tests are very rare in Switzerland. They are well-known around the world at companies like Google, or at Swisscom in Switzerland. Some of the 450 applicants also include major players in the IT scene, with plenty of skill in this area. Registration is mandatory in order to protect other applications on the Swiss Post server against unauthorized hacking attempts. This is also set out in the Code of Conduct. Hacking into systems is a punishable offence in Switzerland, which means that agreements have to be place to protect the hackers accordingly.

How does type of endurance test for e-voting security precautions work? What is the exact procedure?

Using our system, we simulate a ballot contest with the usual time frame of four weeks. This includes sending out voting cards, casting votes and counting the results. The test therefore resembles a regular ballot contest. During this period, the hackers can let loose with several voting cards in the e-voting system. Their task is to try to manipulate the ballot box without us noticing.

What does Swiss Post expect from this public hacker test? Don't the Federal Chancellery's security requirements already conform to the strictest standards in the world at present?

The high level of security is provided by an overall concept encompassing all the technology used and not by a single measure or piece of software. Our e-voting system meets the very strict security requirements. In a very simplified (and figurative) sense, it can be seen as a sort a hedgehog, which rolls up defensively by reflex. Any fox that tries to make a grab for the hedgehog will find himself with a bloody nose full of spines and little chance of success. Unless the fox, a master of survival with his cunning plans and clever behaviour, finds a way to outsmart the hedgehog. We

are applying the same method in the hope of gaining insight and knowledge into the ideas, imagination, intelligence and scenarios the sly hacker will use to attack our system – our "hedgehog" – without receiving a bloody nose.

You are promising an even higher level of security than is used in online banking systems, which are now an everyday part of life. All thanks to the concepts of "individual and universal verifiability". What does this mean for me, as a layperson?

Well, the arguments against e-voting are mostly based on emotions instead of facts – the intrusion test is designed to facilitate a fact-oriented discussion. It should show that the precautions in the sensitive sphere of digital voting and elections have become so effective that any form of manipulation can be immediately identified, which is not the case for existing voting processes. Individual verifiability means that voters receive a series of numbers as confirmation from the system that their vote has landed in the ballot box as they intended. If the number series they receive does not match the series on their voting card, they can identify that someone has attempted to manipulate their vote as it enters the ballot box.

…and universal verifiability?

As a system, universal verifiability provides conclusive proof that the ballot box has been correctly counted. We have undertaken security precautions along the vote's entire digital route, from the moment it is placed in the ballot box right through to the counting process. These precautions ensure that any attempt at manipulation is reported either to the voter or to the relevant canton.

Swiss Post publishes today the source code. What does this mean exactly? What insight will this give to the IT experts?

The electronic ballot box consists of various technical components. These include a piece of software featuring all the cryptographical elements, such as encryption and verifiability. The source code shows how the software has been written and how it works. Metaphorically speaking, the source code is the recipe, which states and describes the required infrastructure. It gives the "cooks" a look at the recipe. Whether they can use their skills to recreate the menu as well as the person who wrote the recipe remains to be seen. As you can see, a great deal of information is being disclosed. This is also important because only with transparency can we establish the trust necessary to implement a digital voting/election process in the future.

Are you willing to give us your forecast of the stress test in February?

We are keen to see the creativity, sophistication and versatility of the hackers and how they use these skills when putting our e-voting system to the test. But it is not simply a question of which problem-solving approach will be selected; it is more about discovering whether the system can reliably detect attempts at manipulation and raise the alarm.

What reward will be given to hackers who manage to prove to Swiss Post that there are loopholes?

We anticipate a total sum of CHF 150,000 to compensate for any expenses incurred. This will be awarded on a sliding scale up to a maximum amount of CHF 50,000 depending on success and recommendation.

Issued by the Swiss Confederation and cantons

Today (Thursday), the Swiss Confederation and cantons are publishing a press release (link (https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73898.html)) announcing another milestone on the path to an e-voting system in Switzerland: in accordance with the requirements of federal law, an e-voting system with complete verifiability must be subjected to a public intrusion test prior to being used for the first time. This test verifies security by allowing the system to be attacked. Swiss Post will be implementing these directives by running a planned public intrusion test from mid-February.
Swiss Post welcomes this approach. This process supports a fact-based public discussion on issues of security. It will be the responsibility of the cantonal parliaments and the Swiss public to decide whether to introduce e-voting as a third, additional channel alongside the ballot box and postal voting.
Swiss Post currently transports around 20 million letter consignments via the postal channel solely for elections and votes.

Further information:

e-voting-Blog: Public hacker test (https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system)

e-voting-Blog: Source code (https://www.evoting-blog.ch/en/pages/2019/swiss-post-publishes-the-source-code-for-its-e-voting-system)

Registration for the intrusion test: www.onlinevote-pit.ch (http://www.onlinevote-pit.ch/)

Swiss Confederation: (https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html)intrusion test (https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html)

Categorised in:

Delivery (https://post-medien.ch/en/category/delivery/),
General (https://post-medien.ch/en/category/general/),
Innovations (https://post-medien.ch/en/category/innovations/),
Letters (https://post-medien.ch/en/category/letters/),
Policy (https://post-medien.ch/en/category/policy/),

(https://post-medien.ch/en/swiss-posts-voting-system-put-through-its-paces-by-hackers/?share=email&nb=1)

Related Posts

Berne: the heart of the world's postal service

(https://post-medien.ch/en/berne-the-heart-of-the-worlds-postal-service/)
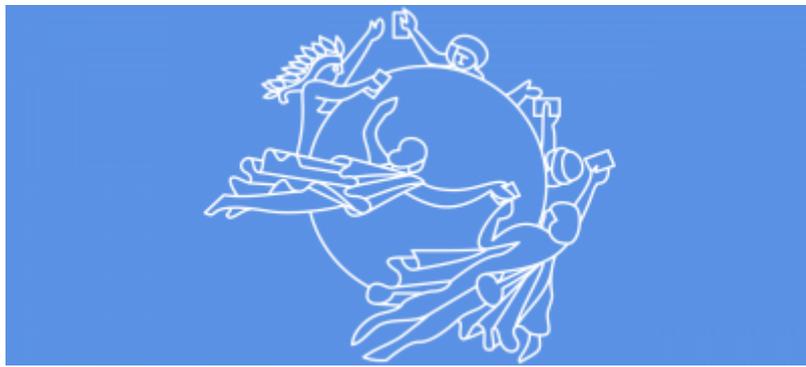
by **Erich Goetschi (https://post-medien.ch/en/author/goetschier/)** 9. October 2019

Contact

Tel.: +41 58 341 00 00 (tel:+41583410000)
Tel. (on call): +41 79 322 74 41 (tel:+41583410000) (in emergencies outside office hours)
E-mail: presse@swisspost.ch (mailto:presse@swisspost.ch)
News and information on Twitter: @swisspostnews_e (https://twitter.com/swisspostnews_e)

At Swiss Post, Christmas starts at the end of November

(https://post-medien.ch/en/at-swiss-post-christmas-starts-at-the-end-of-november/)

by (https://www.facebook.com/swisspost)

Léa Wertheimer (https://post-medien.ch/en/author/leawertheimer/)
19. November 2018

Follow Us

(https://www.facebook.com/swisspost) 🐦 (https://twitter.com/PostSchweiz)
(https://www.instagram.com/swisspost/) ▶ (http://www.youtube.com/swisspost)
in (https://www.linkedin.com/company/swiss-post)
X (https://www.xing.com/companies/dieschweizerischepost)

RSS Feed

(https://post-medien.ch/en/feed/)

Accessibility (https://www.post.ch/en/pages/footer/accessibility-at-swiss-post)

General Terms and Conditions (https://www.post.ch/en/pages/footer/general-terms-and-conditions-gtc)

Data protection and disclaimer (https://www.post.ch/en/pages/footer/data-protection-and-disclaimer)

Publication details (https://www.post.ch/en/pages/footer/publication-details)