Statement on recent comments regarding the source code publication of the Swiss e-voting system

Scytl

Barcelona, February 22, 2019 – Following the requirements of the Confederation and Cantons, Swiss Post and Scytl recently published the source code and cryptographic protocols of the e-voting system used in Switzerland, in order to allow researchers and other stakeholders with interest to share constructive feedback on the code and protocol design.

The source code of the Swiss e-voting system has been published in an official repository managed by Swiss Post in Gitlab, which also offers an official channel to provide feedback. Access to this official repository and communication channel is subject to a source code access agreement. Scytl welcomes any person interested to share their comments on GitLab and will be eager to reply to them.

However, Scytl has detected parallel unofficial repositories of presumably the same source code that also triggered the creation of other discussions threads. In such cases, it is impossible to guarantee the integrity and authenticity of any source code hosted in unofficial repositories as well as the validity of their related comments. Scytl will therefore only respond to comments and questions submitted through the official channel. Hundreds of researchers and other stakeholders have already agreed to use the formal source code repository and its corresponding access agreement as well as using the official channel to share feedback in a constructive way. At this point, no vulnerability has been found in the cryptographic protocols, which constitutes a paradigm for the e-voting system security.

Unfortunately, over the last days, several comments were made by some individuals outside the official channel, claiming that the cryptographic protocols were not secure and making general comments on the quality of the code. Comments made in unofficial threads do not allow to build a comprehensive and constructive dialogue on the source code, and do not serve the security community or the citizens interest.

These criticisms are mainly based on misunderstandings related to the cryptographic mechanisms, which have already been clarified and solved in the official repository. The cryptographic protocols and mechanisms implemented in the code are very advanced and not commonly found in other software. This may make the analysis more complex for some of the individuals evaluating and posting public comments, who, in turn, foster misunderstandings and may generate confusions.

The cryptographic protocols and their related computational and symbolic proofs, published jointly to the source code, tangibly demonstrate the compliance of the e-voting system with the privacy and complete verifiability requirements established by the Swiss Chancellery.

These protocols are the result of the research carried out since the foundation of Scytl in 2001, which has been made available to the public through ongoing academic publications. They have successfully passed the scrutiny of 3rd party cryptographic experts.

It is indeed because the cryptographic protocols have achieved complete verifiability that the source code has been published, with the confidence that no attack might compromise the secrecy of the ballot box and the integrity of the election results.

We do encourage researchers to use the official repository in order to (i) share information and (ii) avoid multiple answers on the same findings.

Unofficial communication channels could be based on incorrect analysis or could use untrusted source code repositories. They cannot be trusted and do not contribute to building a transparent and trust environment around e-voting.

Swiss Post and Scytl will be subjecting their fully verifiable e-voting system to a public intrusion test, starting February 25th where researchers and other stakeholders can test the system in a real environment. Register is open at https://www.onlinevote-pit.ch/.