A privacy attack on the Swiss Post e-voting system

Véronique Cortier, Alexandre Debant, and Pierrick Gaudry

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

Amsterdam, April 13th 2022
Launch of the « electronic vote » projet


A brief history

Launch of the "electronic vote" projet

Revision of the federal law

A brief history

Launch of the « electronic vote » projet
Revision of the federal law
First trial in Geneva
Neuchatel + Zurich
Basel-Stadt + Lucerne + Bern
Trials in 14 cantons

A brief history

Launch of the « electronic vote » projet

Revision of the federal law

First trial in Geneva

Neuchatel + Zurich

50% of Swiss abroad can vote online in federal elections

Basel-Stadt + Lucerne + Bern

Trials in 14 cantons


50% of Swiss abroad can vote online in federal elections

A brief history

Launch of the « electronic vote » projet

Revision of the federal law

First trial in Geneva

Neuchâtel + Zurich

50% of Swiss abroad can vote online in federal elections

Basel-Stadt + Lucerne + Bern

50% of cantonal electorate can vote with the Swiss Post solution

Trials in 14 cantons


Launch of the « electronic vote » projet 2000
Revision of the federal law 2003
First trial in Geneva 2005
Neúchatel + Zurich
Basel-Stadt + Lucerne + Bern
50% of Swiss abroad can vote online in federal elections 2009
50% of cantonal electorate can vote with the Swiss Post solution 2012
Trials in 14 cantons 2015
2017
2019
Public release of the system… attack found… E-voting is stopped.

Today… and tomorrow…

Revision of the Federal Chancellery
Ordinance on Electronic voting (VEleS)

1 July 2018

- Art. 7a Publication of the source code

1 The source code for the system software must be made public.

5.1.1 Examination criteria: The protocol must meet the security objective according to the trust assumptions in the abstract model in accordance with Section 4. In addition, a cryptographic and a symbolic proof must be provided. The proofs relating to cryptographic basic components may be provided according to generally accepted security assumptions (for example, the "random oracle model", "decisional Diffie-Hellman assumption", "Fiat-Shamir heuristic"). The protocol should be based if possible on existing and proven protocols.

https://www.fedlex.admin.ch/eli/cc/2013/859/en
Today... and tomorrow...

1 July 2018
Revision of the Federal Chancellery Ordinance on Electronic voting (VEleS)

21 Dec. 2020
Federal Council launches redesign of trials

05 July 2021
Federal government launches examination of new e-voting system

10 Dec. 2021
New legal basis for e-voting (to be finalized by mid-2022)

Sept. 2022
Federal elections including e-voting

---

Art. 7a
Publication of the source code

The source code for the system software must be made public.

---

5.1.1 Examination criteria: The protocol must meet the security objective according to the trust assumptions in the abstract model in accordance with Section 4. In addition, a cryptographic and a symbolic proof must be provided. The proofs relating to cryptographic basic components may be provided according to generally accepted security assumptions (for example, the "random oracle model", "decisional Diffie-Hellman assumption", "Fiat-Shamir heuristic"). The protocol should be based if possible on existing and proven protocols.

---

https://www.fedlex.admin.ch/eli/cc/2013/859/en
Swiss-Post system

Context:
- Swiss Post bought Scytl’s solution in 2019 (ALEX?)
- Fixed vulnerabilities
- Improved the code and the specification
Swiss-Post system

**Context:**
- Swiss Post bought Scytl’s solution in 2019 (ALEX?)
  - Fixed vulnerabilities
  - Improved the code and the specification

We have been contacted to update the symbolic proofs of the systems.
Swiss-Post system

**Context:**
- Swiss Post bought Scytl’s solution in 2019 (ALEX?)
- Fixed vulnerabilities
- Improved the code and the specification

---

We have been contacted to update the symbolic proofs of the systems.

---

There is a vote secrecy attack: an attacker can learn the vote of everyone!
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server

ballot
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server

- ballot
- return code
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server

- ballot
- return code
- ok
Overview of the system

- Print Office
- 4 Control Components (CCRs)
- Voting Server
- Judge / Auditors
- 4 Mixing Control Components (CCMs)

Diagram flows:
- ballot
- return code
- ok
Overview of the system

Print Office

4 Control Components (CCRs)

Judge / Auditors

Voting Server

4 Mixing Control Components (CCMs)

Print Office

4 Control Components (CCRs)

Judge / Auditors

Voting Server

4 Mixing Control Components (CCMs)
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server

4 Mixing Control Components (CCMs)

Judge / Auditors

ballot
return code
ok
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server

4 Mixing Control Components (CCMs)

Judge / Auditors
Overview of the system

Print Office

4 Control Components (CCRs)

Judge / Auditors

Voting Server

4 Mixing Control Components (CCMs)
Overview of the system

Print Office

4 Control Components (CCRs)

Voting Server

Judge / Auditors

4 Mixing Control Components (CCMs)

Print Office

4 Control Components (CCRs)

Voting Server

Judge / Auditors

4 Mixing Control Components (CCMs)
Vote secrecy - no one is able to learn who I voted for!

Graph showing two voters, one voting 0 and the other voting 1, with the statement that these votes are equivalent.
Vote secrecy

Vote secrecy - no one is able to learn who I voted for!

Federal chancellerie requirements:

2.9.3.1 The following system participants are regarded as untrustworthy:
- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters

2.9.3.2 The following system participants may be considered trustworthy:
- set-up component
- print component
- user device
- one of four control components per group, leaving open which one it is
- one auditor in any group, leaving open which auditor it is; Number 2.7.2 takes precedence
Vote secrecy

Vote secrecy - no one is able to learn who I voted for!

Federal chancellorie requirements:

2.9.3.1 The following system participants are regarded as untrustworthy:
- UT system
- three of four control components per group, leaving open which three they are
- a significant proportion of voters

2.9.3.2 The following system participants may be considered trustworthy:
- set-up component
- print component
- user device
- one of four control components per group, leaving open which one it is
- one auditor in any group, leaving open which auditor it is; Number 2.7.2 takes precedence

Vote secrecy

Vote secrecy - no one is able to learn who I voted for!

I vote 0  I vote 1  ≈  I vote 1  I vote 0

Federal chancellery requirements:

2.9.3.1 The following system participants are regarded as untrustworthy:
   - UT system
   - three of four control components per group, leaving open which
     three they are
   - a significant proportion of voters

2.9.3.2 The following system participants may be considered trustworthy:
   - set-up component
   - print component
   - user device
   - one of four control components per group, leaving open which one it
     is
   - one auditor in any group, leaving open which auditor it is; Number
     2.7.2 takes precedence

Few details about the actual implementation.

Print Office -> 4 Control Components (CCRs) -> Voting Server

ballot
return code
ok

Judge / Auditors

4 Mixing Control Components (CCMs)
Few details about the actual implementation
Few details about the actual implementation
Few details about the actual implementation.
A vote secrecy attack

Print Office
4 Control Components (CCRs)

Voting Server

Lucerne

Bern

Zürich

Judge / Auditors

Print Office
4 Control Components (CCRs)

Voting Server

4 Mixing Control Components (CCMs)
A vote secrecy attack

The attacker introduces a fake ballot-box

4 Mixing Control Components (CCMs)
A vote secrecy attack

The attacker introduces a fake ballot-box

The 3 malicious CCM do not generate the proof for the fake ballot-box
A vote secrecy attack

The attacker introduces a fake ballot-box

The 3 malicious CCM do not generate the proof for the fake ballot-box

The attacker learns Alice’s vote

Judge / Auditors

4 Mixing Control Components (CCMs)
Impact of the attack

In theory: the attacker can learn the vote of all the voters
Impact of the attack

**In theory:** the attacker can learn the vote of all the voters

**In practice without being detected:**
- he cannot add too many fake ballot-boxes
- can learn the vote of at most $k$ voters
- but $k$ might be relatively large because fake ballot-boxes are very small (one ballot)

It would introduce a detectable overhead in the computation time
Impact of the attack

**In theory:** the attacker can learn the vote of all the voters

**In practice without being detected:**
- he cannot add too many fake ballot-boxes
- can learn the vote of at most $k$ voters
- but $k$ might be relatively large because fake ballot-boxes are very small (one ballot)

**In practice being detected:**
- same things as presented on the left
- he can learn the vote of at least $n$ voters (where $n$ is the number of counting circle)

the auditor does not check it’s received enough proofs before revealing the last key

it would introduce a detectable overhead in the computation time
Impact of the attack

**In theory:** the attacker can learn the vote of all the voters

**In practice without being detected:**
- he cannot add too many fake ballot-boxes
- can learn the vote of at most $k$ voters
- but $k$ might be relatively large because fake ballot-boxes are very small (one ballot)

**In practice being detected:**
- same things as presented on the left
- he can learn the vote of at least $n$ voters
  (where $n$ is the number of counting circle)
- the auditor does not check it’s received enough proofs before revealing the last key

**According to Swiss Post and the Chancellerie:** it is a critical flaw that must be fixed!
Many similar attack scenarios can be derived from ours.
How to fix the attack?

1. A weak counter-measure:
   - set the number $n_B$ of ballot-boxes as a public parameter of the election
   - ensure that the CCMs check they decrypt at most $n_B$ ballot-boxes
   - ensure that the judge/auditor has received exactly $n_B$ proofs before revealing the last key
How to fix the attack?

1. A weak counter-measure:
   - set the number $n_B$ of ballot-boxes as a public parameter of the election
   - ensure that the CCMs check they decrypt at most $n_B$ ballot-boxes
   - ensure that the judge/auditor has received exactly $n_B$ proofs before revealing the last key

2. A stronger counter-measure:
   - implement 1.
   - require that each CCMs recomputes the initial payloads (i.e. the content of the initial ballot-box)
   - require that each CCMs verifies all the previous proofs of correct mixing/decryption

   ➡ These two requirement are quite expensive…
Conclusion

This attack will be fixed in a future release of the specification/implementation

Today, the Swiss Post solution provides a very high level of security. with a high level of transparency, and many expert audits
This attack will be fixed in a future release of the specification/implementation

Lesson learned
It is important to model all the specificities of the system when we do formal proofs (symbolic or computational ones)
e.g. multi ballot-boxes or elections scenarios

Today, the Swiss Post solution provides a very high level of security.
with a high level of transparency, and many expert audits
Conclusion

This attack will be fixed in a future release of the specification/implementation

Lesson learned
It is important to model all the specificities of the system when we do formal proofs (symbolic or computational ones)
e.g. multi ballot-boxes or elections scenarios

Today, the Swiss Post solution provides a very high level of security.
with a high level of transparency, and many expert audits

Future work
The Federal Chancellerie requirements will continue to evolve…
Let’s keep on working to be sure that they remain coherent and that the Swiss Post solution (and others) satisfies them.