The Adventurous Tale of Online Voting in Switzerland

Christian Folini / @ChrFolini

OWASP BE - 2021-03-18
Voting in Switzerland

Photo: Gian Ehrensberger
### Wahl von 7 Mitgliedern des Grossen Rats
vom 18. Oktober 2020

**Kanton Aargau**

<table>
<thead>
<tr>
<th>Nummer</th>
<th>Kandidat / Kandidatin</th>
<th>Stimmkreis</th>
</tr>
</thead>
<tbody>
<tr>
<td>06.01</td>
<td>Budmiger Hans-Peter (Hampi), 1976, Unternehmer, Gemeindepräsident, Muri</td>
<td></td>
</tr>
<tr>
<td>06.02</td>
<td>Langenbacher Knüsel Silvia, 1966, Unternehmerin, Abtwill</td>
<td></td>
</tr>
<tr>
<td>06.03</td>
<td>Payer Samuel, 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri</td>
<td></td>
</tr>
<tr>
<td>06.04</td>
<td>Meusser Loredana, 1996, Blaw Masterstudentin Rechtswissenschaften, Waltenswil</td>
<td></td>
</tr>
<tr>
<td>06.05</td>
<td>Stöckli Cornel, 1975, Dr. med., Rheumat. &amp; Innere Med., Integrationskom., Muri</td>
<td></td>
</tr>
<tr>
<td>06.06</td>
<td>Chande Sabrina, 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil</td>
<td></td>
</tr>
<tr>
<td>06.07</td>
<td>Weber Thomas, 1974, Content Manager, Journalist, Buttwil</td>
<td></td>
</tr>
</tbody>
</table>

**Wahlzettel-Nr.**

**Bezirk**

Muri

---

**Vom Wahlbüro auszufüllen**: | **Kandidatenstimmen**: | **Zusatzstimmen**: | **Total**: |
---|---|---|---|

Typical Swiss Election Ballot

Bonus points for spotting the content manager from Butt-ville.
"We simply can’t build an Internet voting system that is secure against hacking because of the requirement for a secret ballot."

Bruce Schneier, Online Voting Won’t Save Democracy, The Atlantic, May 2017
Arguments in Favor of Internet Voting

The Swiss Perspective
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad

- Visually impaired and quadriplegic voters
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad
- Visually impaired and quadriplegic voters
- Formally invalid ballots
Arguments in Favor of Internet Voting

The Swiss Perspective

- Citizens living abroad
- Visually impaired and quadriplegic voters
- Formally invalid ballots
- Security issues of physical voting
The Cantons of Switzerland

1st Swiss internet voting project is launched with three pilot cantons.

1st project

2000

Canton Geneva runs the first Swiss internet voting trial.

1st Geneva trial

2004

Swiss expats are allowed to vote via Scytl internet voting system in canton Neuchâtel.

Entering Scytl

2008

Federal administration and cantons establish a joint steering committee.

Steering Board

2009

Eight Swiss cantons form a consortium and commission Unisys with the creation of an internet voting system.

Consortium

2011
Federal administration and cantons establish a joint steering committee.

**2011**

- **Steering Board**

**2015**

- **Consortium dies**

  The eight consortium cantons throw towel after federal administration bars system from use in national elections.

**2016**

- **Scytl/Swiss Post join**

  Spanish Scytl and Swiss Post form joint venture and go into production.

**2017**

- **Mainstreaming attempt**

  The federal chancellor calls for 2/3 of the cantons to offer internet voting for national elections in 2019.
Geneva Quits

2018: Development stopped
2019: System terminated

Source: Twitter: @GE_chancellerie (1141332323025195009)
Spanish Scytl and Swiss Post form joint venture and go into production.

**Scytl/Swiss Post join**

2016

**Mainstreaming attempt**

The federal chancellor calls for 2/3 of the cantons to offer internet voting for national elections in 2019.

2017

**Geneva quits**

Political quarrels lead to Geneva stopping all further development. A year later, the system is terminated.

2018

**Source Code Publication**

Scytl / Swiss Post publish the source code of their system and run a 4 week bug bounty

2019
Swiss Post Bug Bounty: We got this!

Abschlussbericht Öffentlicher Intrusionstest

Div Post

1. Best Practices
   - 16 Befunde

2. Intrusion into the system
   - 0 Befunde

3. Destruction of votes / Rendering the votes in the digital urn useless
   - 0 Befunde

4. Breaking vote secrecy within the system
   - 0 Befunde

5. Detectable vote manipulation
   - 0 Befunde

6. Undetectable vote manipulation
   - 0 Befunde

[BEST PRACTICES] Incorrect 'HTTP-Strict-Transport-Security' header on 'pit-admin.evoting-test.ch'

REDMINE ID: #188
SUBMISSION: Feb. 25th 2019, 23:19 (GMT+1)
RESEARCHER(S): Jacob Rees-Earcher
COMPENSATION: CHF 200

When connecting to 'pit-admin.evoting-test.ch' on port 443, the server sends an HTTP-Strict-Transport-Security header even for plaintext HTTP connections, which is a violation of RFC 6797. The additional header also does not contain the 'includeSubdomain' directive, which would be a security best-practice.

[BEST PRACTICES] Use of 'unsafe-eval' and 'unsafe-inline' in Content Security Policy

[BEST PRACTICES] Multiple occurrences of 'X-XSS-Protection' HTTP header

REDMINE ID: #234
SUBMISSION: Feb. 28th 2019, 14:57 (GMT+1)
RESEARCHER(S): pitbull
COMPENSATION: CHF 100

Some error messages sent as responses by the web server (specifically, the '403 Forbidden' status code) include two identical occurrences of the 'X-XSS-Protection' security header. This behavior is non-standard, and could lead to undefined behavior in some browsers.
Swiss Post / Scytl Source Code: Not so good

The trapdoor-commitment issue in the Swiss e-voting system was also independently discovered by Thomas Haines of NTNU and by Rolf Hauri of Bern University of Applied Sciences. — @SarahJamieson

The Register

Security

Swiss electronic voting system like... wait for it, wait for it... Swiss cheese: Hole found amid public source code audit

Hey, at least it was dis – which is the whole p

By Thomas Claburn in San Francisco

Sarah Jamieson Lewis @SarahJamiesonLewis - 12 Mârz 2019
It is 9am Swiss Time, @VTweedacan. Olivier Pereira & I are releasing details of a cryptographic trapdoor that we found in the Swiss Post #voting system that would allow admins to falsely “prove” that votes were undetectably compromised elections people.org.unimelb.edu.au/vt/election/swiss....

The Daily Swig

Cybersecurity news and views

Swiss Post puts e-voting on hold after researchers uncover critical security errors

Vanessa Teague @VTweedacan - 11 April 2019
I agree with @demonism on the safety of paper ballots in Aus elections, but the electronic Senate count opens the possibility for undetected error or fraud unless there’s a rigorous public audit of the paper records against the digitised preferences. arxiv.org/abs/1610.00127 twitter.com/GeoffreyHPowell...

Researchers Find Critical Backdoor in Swiss Online Voting System

und a severe issue in the new Swiss internet they say would let someone alter votes y it should put a halt to Switzerland’s plan to roll elections this year.

Vanessa Teague @VTweedacan - 11 April 2019
@SarahJamieson, Olivier Pereira & I found serious cryptographic errors in Scytl’s Swiss/NZV evoting system. Will Scytl’s Aus Senate counting code remain secret and will it enter votes into the count without a public audit of our paper ballots?
tenders.gov.au/?event=public....

to be continued ...
Spanish Scytl and Swiss Post form joint venture and go into production.

**Scytl/Swiss Post join**

2016

Political quarrels lead to Geneva stopping all further development. A year later, the system is terminated.

**Geneva quits**

2018

The steering board establishes a dialog with 25 scientists to assess viability of internet voting and support with writing new regulation.

**Rebooting**

2019

The federal chancellor calls on 2/3 of the cantons to offer internet voting for national elections in 2019.

**Mainstreaming attempt**

2017

Scytl / Swiss Post publish the source code of their system. Researchers identify three critical vulnerabilities within weeks. The system is put on hold.

**Source Code Publication**

2020
Expert Dialogue – Participating Scientists

CRYPTOGRAPHERS AND ONLINE VOTING EXPERTS
- David Basin, ETH Zurich
- Srdjan Capkun, ETH Zurich
- Eric Dubuis, BFH Bern
- Bryan Ford, EPF Lausanne
- Reto Koenig, BFH Bern
- Philipp Locher, BFH Bern
- Olivier Pereira, University of Leuven, Belgium
- Vanessa Teague, Australia
- Bogdan Warinschi, Bristol, UK
- Rolf Haenni, BFH Bern

SECURITY INDUSTRY
- Stéphane Adamiste, SCRT
- Sergio Alves Domingues, SCRT
- Tobias Ellenberger, One Consult

COMPUTER SCIENTISTS
- David-Olivier Jaquet-Chiffelle, University of Lausanne
- Oscar Nierstrasz, University of Bern
- Adrian Perrig, ETH Zurich
- Carsten Schürmann, Denmark
- Matthias Stürmer, University of Bern
- Ulrich Ultes-Nitsche, University of Fribourg

POLITICAL SCIENTISTS
- Florian Egloff, ETH Zurich
- Fabrizio Gilardi, University of Zurich
- Uwe Serdült, Center for Democracy, Aarau

MODERATOR
- Christian Folini, netnea.com

Source: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html
Expert Dialogue – Participating Scientists

CRYPTOGRAPHERS AND ONLINE VOTING EXPERTS
- David Basin, ETH Zurich
- Srdjan Capkun, ETH Zurich
- Eric Dubuis, BFH Bern
- Bryan Ford, EPF Lausanne
- Reto Koenig, BFH Bern
- Philipp Locher, BFH Bern
- Olivier Pereira, University of Leuven, Belgium
- Vanessa Teague, Australia
- Bogdan Warinschi, Bristol, UK
- Rolf Haenni, BFH Bern

SECURITY INDUSTRY
- Stéphane Adamiste, SCRT
- Sergio Alves Domingues, SCRT
- Tobias Ellenberger, One Consult

COMPUTER SCIENTISTS
- David-Olivier Jaquet-Chiffelle, University of Lausanne
- Oscar Nierstrasz, University of Bern
- Adrian Perrig, ETH Zurich
- Carsten Schürmann, Denmark
- Matthias Stürmer, University of Bern
- Ulrich Ultes-Nitsche, University of Fribourg

POLITICAL SCIENTISTS
- Florian Egloff, ETH Zurich
- Fabrizio Gilardi, University of Zurich
- Uwe Serdült, Center for Democracy, Aarau

MODERATOR
- Christian Folini, netnea.com

Source: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html
Expert Dialogue – Participating Scientists

CRYPTOGRAPHERS AND ONLINE VOTING EXPERTS
David Basin, ETH Zurich
Srdjan Capkun, ETH Zurich
Eric Dubuis, BFH Bern
Bryan Ford, EPF Lausanne
Reto Koenig, BFH Bern
Philipp Locher, BFH Bern
Olivier Pereira, University of Leuven, Belgium
Vanessa Teague, Australia

SECURITY INDUSTRY
Stéphane Adamiste, SCRT
Sergio Alves Domingues, SCRT
Tobias Ellenberger, One Consult

COMPUTER SCIENTISTS
David-Olivier Jaquet-Chiffelle, University of Lausanne
Oscar Nierstrasz, University of Bern
Adrian Perrig, ETH Zurich
Carsten Schürmann, Denmark
Matthias Stürmer, University of Bern
Ulrich Ultes-Nitsche, University of Fribourg

POLITICAL SCIENTISTS
Florian Egloff, ETH Zurich
Fabrizio Gilardi, University of Zurich
Uwe Serdült, Center for Democracy, Aarau

MODERATOR
Christian Folini, netnea.com

Source: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html
The dialogue starts with a survey over 62 questions sent to 25 scientists.

**Survey**

Covid-19 hits

When the on-site workshops were slowly taking shape, Switzerland entered a lockdown and the on-site gatherings had to be called off.

**2020.2**

Online dialogue

The workshops are replaced with a 12 weeks online dialogue on a dedicated gitlab platform.

**2020.4**

Scientific report

The steering board publishes the 70 pages report with the recommendations of the scientists.

**2020.11**

Additional research

Several separate research articles are commissioned with individual scientists to bring up more information on individual questions.
Key Recommendations of Dialogue
Key Recommendations of Dialogue

- Strict hierarchy of specifications
Key Recommendations of Dialogue

- Strict hierarchy of specifications
- Diversity in hard- and software
Key Recommendations of Dialogue

- Strict hierarchy of specifications
- Diversity in hard- and software
- Maximum level of transparency, namely in development
Key Recommendations of Dialogue

- Strict hierarchy of specifications
- Diversity in hard- and software
- Maximum level of transparency, namely in development
- Voting security beyond internet voting
Summary

- Switzerland is a useful test bed for online voting
- Iterative process with strict supervision on federal level
- Expert dialogue with recommendations in 2020

Contact

Christian Folini

christian.folini@netnea.com

@ChrFolini

Download English version of report from