

Belenios: the Certification Campaign

A. Bossuat, E. Brocas, V. Cortier, P. Gaudry, S. Glondu, N. Kovacs

whoami



 Angèle Bossuat

 R&D engineer at Quarkslab

 Cryptography

Context



Quarkslab engineers conducted a CSPN evaluation of Belenios, the e-voting solution designed by LORIA researchers.

We present our work, and future perspectives.



Table of Contents

Belenios and e-Voting

Belenios + CSPN = ?

Fitting Belenios in a CSPN

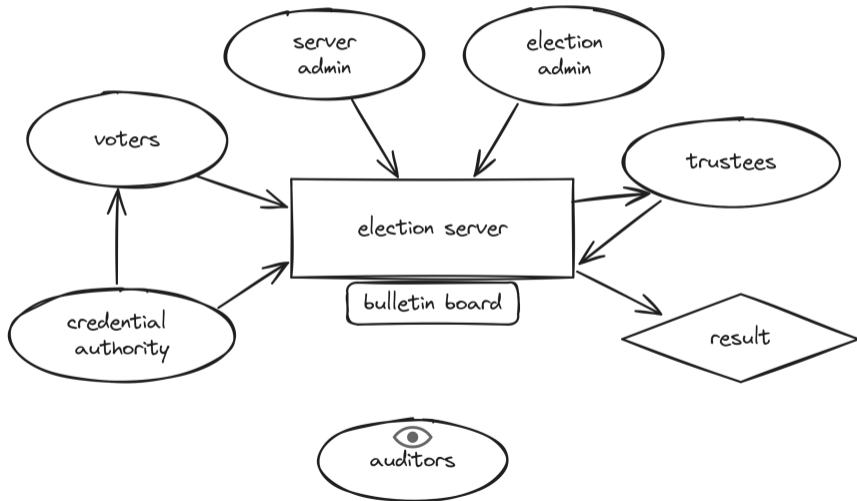
Evaluating Belenios in a CSPN

Takeaway

Belenios = Hélios  + Belenos 

- ▶ internet voting system created by LORIA researchers
- ▶ over ten years old, still maintained
- ▶ new features added regularly
- ▶ election can be setup on the LORIA server, or self-hosted

Parties and roles



Security properties



Academia: analyzed as a protocol, not a software.



Security properties



Academia: analyzed as a protocol, not a software.

Ballot not modified, secret, only legit votes





Security properties

Academia: analyzed as a protocol, not a software.

Ballot not modified, secret, only legit votes

Voters legitimate voters, can check their ballot is cast





Security properties

Academia: analyzed as a protocol, not a software.

Ballot not modified, secret, only legit votes

Voters legitimate voters, can check their ballot is cast


Auditors check voting client, check result





Security properties

Academia: analyzed as a protocol, not a software.

Ballot	not modified, secret, only legit votes
Voters	legitimate voters, can check their ballot is cast
Auditors	check voting client, check result
Coercion	not protected 





- ▶ The CNIL¹ has guidelines for internet voting
 - ▶ no clear trust model (e.g. w/ the server)
 - ▶ no open-sourcing recommendation
 - ▶ against internet voting for political elections

¹Commission Nationale de l'Informatique et des Libertés



e-Voting Facts

- ▶ The CNIL¹ has guidelines for internet voting
 - ▶ no clear trust model (e.g. w/ the server)
 - ▶ no open-sourcing recommendation
 - ▶ against internet voting for political elections
- ▶ Switzerland: very demanding regulations, precise model, transparency, bug bounties
 - ▶ flaws discovered in 2019, suspension of e-voting until 2023

¹Commission Nationale de l'Informatique et des Libertés



e-Voting Facts

- ▶ The CNIL¹ has guidelines for internet voting
 - ▶ no clear trust model (e.g. w/ the server)
 - ▶ no open-sourcing recommendation
 - ▶ against internet voting for political elections
- ▶ Switzerland: very demanding regulations, precise model, transparency, bug bounties
 - ▶ flaws discovered in 2019, suspension of e-voting until 2023
- ▶ Estonia, Australia: more or less transparent, severe flaws discovered

¹Commission Nationale de l'Informatique et des Libertés



e-Voting Facts

- ▶ The CNIL¹ has guidelines for internet voting
 - ▶ no clear trust model (e.g. w/ the server)
 - ▶ no open-sourcing recommendation
 - ▶ against internet voting for political elections
- ▶ Switzerland: very demanding regulations, precise model, transparency, bug bounties
 - ▶ flaws discovered in 2019, suspension of e-voting until 2023
- ▶ Estonia, Australia: more or less transparent, severe flaws discovered
- ▶ France: flawed solution for abroad voters in the '22 legislatives
 - ▶ A. Debant et L. Hirschi / USENIX '23 or NoLimitSecu#454

¹Commission Nationale de l'Informatique et des Libertés



Table of Contents

Belenios and e-Voting

Belenios + CSPN = ?

Fitting Belenios in a CSPN

Evaluating Belenios in a CSPN

Takeaway



What is a CSPN?

Certification de Sécurité Premier Niveau
First Level Security Certification








-  35 days = 25 for technical evaluation + 10 for cryptography
-  analyze conformity, and evaluate the strength of security functions
-  *sponsor* provides the *ITSEF* with the Security Target and Crypto Mechanisms
-  ITSEF provides a report
-  after restitution, the ANSSI decides to deliver the certification  or not 



Table of Contents

Belenios and e-Voting

Belenios + CSPN = ?


- Fitting Belenios in a CSPN

- Evaluating Belenios in a CSPN

Takeaway

Security Functions



-  **vote privacy** protects against *vote divulcation*
 - ▶ vote encryption, shared key, verifiable voting client



Security Functions



vote privacy protects against *vote divulgation*




- ▶ vote encryption, shared key, verifiable voting client



result confidentiality protects against *early result divulgation*

Security Functions



-  **vote privacy** protects against *vote divulgation*
 - ▶ vote encryption, shared key, verifiable voting client
-  **result confidentiality** protects against *early result divulgation*
-  **result integrity** protects against *result modification*
 - ▶ ballot signature, individual and universal verifiability, answers validity, voters authentication, enhanced verifications

Attacker model



External attacker

Attacker model



External attacker, legitimate voter

Attacker model



External attacker, legitimate voter,
election admin

Attacker model



External attacker, legitimate voter,
election admin, server admin.

Attacker model



External attacker, legitimate voter,
election admin, server admin.

- ▶ credential authority is trusted



Attacker model



External attacker, legitimate voter,
election admin, server admin.

- ▶ credential authority is trusted
- ▶ voters' private credentials are secure

Attacker model



External attacker, legitimate voter,
election admin, server admin.

- ▶ credential authority is trusted
- ▶ voters' private credentials are secure
- ▶ voters' browsers are trusted

Attacker model



External attacker, legitimate voter,
election admin, server admin.

- ▶ credential authority is trusted
- ▶ voters' private credentials are secure
- ▶ voters' browsers are trusted
- ▶ number of dishonest trustees is below the threshold

Attacker model



External attacker, legitimate voter,
election admin, server admin.

- ▶ credential authority is trusted
- ▶ voters' private credentials are secure
- ▶ voters' browsers are trusted
- ▶ number of dishonest trustees is below the threshold
- ▶ at least one honest auditor

Attacker model



External attacker, legitimate voter,
election admin, server admin.

- ▶ credential authority is trusted
- ▶ voters' private credentials are secure
- ▶ voters' browsers are trusted
- ▶ number of dishonest trustees is below the threshold
- ▶ at least one honest auditor
- ▶ admin pages are trusted during setup and tally



Table of Contents

Belenios and e-Voting

Belenios + CSPN = ?

Fitting Belenios in a CSPN

Evaluating Belenios in a CSPN

Takeaway



Vulnerabilities found

Crypto
Web

two non-conformities that were not exploitable ('residual')

one exploited vulnerability, two not exploitable, and *six exploited, but out-of-scope*






- ▶ anyone can upload large files and perform a DoS (but availability is 'out-of-scope')
- ▶ brute-force the verification code and weak CAPTCHA and change the admin password (but web interface is 'out-of-scope')



Target extension




Target too close to academic focus, web not properly handled ► add security functions and threats:

-  **session management**, against *account takeover*
-  **authentication management**, same as above
-  **input validation and sanitization**, against *code injection*



Target extension

Target too close to academic focus, web not properly handled ► add security functions and threats:

-  **session management**, against *account takeover*
-  **authentication management**, same as above
-  **input validation and sanitization**, against *code injection*



This extension resulted into a *failed certification*.
► fix vulnerabilities, evaluate again



Table of Contents

Belenios and e-Voting

Belenios + CSPN = ?

Fitting Belenios in a CSPN

Evaluating Belenios in a CSPN

Takeaway



Key points

- 🔒 saying “it’s not secure” is not sufficient, as it is used in practice
- 📄 we need dedicated frameworks to study e-voting solutions (different attackers, different incentives, specific setups, etc)
- ✓ transparency, precise rules and high expectations work
- 🤝 it’s always important to study both theory and practice

State actors and researchers are open to this discussion, so... let’s go!



Quarkslab: (blog.)quarkslab.com

LORIA: loria.fr