Bern University of Applied Sciences
University of Fribourg

Baloti:
A Verifiable E-Voting System for Immigrants in Switzerland

Stephan Fischli and Oliver Spycher

September 6th, 2010

Outline

Outline

Baloti

- Project conducted by the Zentrum für Demokratie Aarau (interdisciplinary research on democracy)
- Immigrants in Switzerland are limited in their opportunities to be politically active
- Development of an online platform that
  - → contributes to the political integration of immigrants
  - → explains Swiss political processes and disputes
  - → allows immigrants to participate in federal referendums
  - → enables to study the political opinions and the voting behaviour of immigrants
- Supported by the integration fund of the Swiss Confederation

Baloti E-Voting

- Baloti platform integrates an e-voting system
- Immigrants can cast their votes for federal referendums
- The ballots serve a consultative purpose
- Specific usability requirements are
  - → Users are only identified by their e-mail address
  - → Users can join the voter roll at any time and instantly vote
  - → Users should not need to memorize long cryptic values
  - → No client-side installation of software possible

Collaboration

- BFH and ZDA established a partnership within the Baloti project
- Development of the e-voting system "Selectio Helvetica"
- Proof of concept of our verifiable e-voting protocol

Outline

Electronic Channel for Hybrid Systems

- Many governments want to integrate an e-voting channel with their traditional paper-based channel
- Integration as a hybrid system aims at coercion-resistance
  $\rightarrow$ Revoke e-vote and replace it at polling station

Requirements on electronic channel

- Proof of eligibility
- Proof of ownership
- Encryption function allows re-encryption
- Encryption function allows proof of correct re-encryption

PKI Setup for DSA

Voters are assigned their

- private key $s \mod q$
- public key $S = g^s \mod p \qquad (p = 2q + 1)$

Voters can prove that they know the private key (zero-knowledge proof).

Distribution

Voting officials jointly create and publish the public keys and secretly reveal their share of the private key to the voter.

This has to be done only once!

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	Signature of Enc
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_1, g)$
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_2, g)$
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_3, g)$

- Proof of eligibility: simple
- Proof of ownership: simple
- Hugo needs to revoke his vote before casting a paper vote
  1. Choose uniformly random z from $[1, .., q]$
  2. Compute $re\text{-}enc(w_1, z) = (h^{k_1} \cdot h^z, yes \cdot e^{k_1} \cdot e^z)$ and proof
  3. Have polling station authorities sign both
  4. Cast $re\text{-}enc(w_1, z)$, proof and signature to revocation board

What about Privacy?

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (pseudonym generator)
3. Compute pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

Revocation

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

- Proof of eligibility
  1. Hugo reveals his pseudonym $\hat{S}_3$
  2. He proves $ZKP[(s_1) : S_1 = g^{s_1} \wedge \hat{S}_3 = \hat{g}^{s_1}]$
- Proof of ownership: simple
- Revoke encrypted vote: same as in naive version

Properties

- Individual verifiability
- Universal verifiability
- Privacy
- Verifiability of eligibility
- Integrity and accuracy
- Authenticated channel needed only once, i.e. at key generation
- Coercion and vote buying attacks are mitigated by allowing revocation ($\rightarrow$ hybrid system)

Outline

Baloti Specific Requirements

Selectio Helvetica is meant to give the experience of a verifiable voting system that could be used for governmental votes.

We extend the protocol to meet the Baloti specific requirements:

- Users are only identified by their e-mail address
- Users can join the voter roll at any time and instantly vote
- Users should not need to memorize long cryptic values
- No client-side installation of software possible

Selectio Helvetica - Registration

Voters need a password-like voting code for casting votes and individual verifiability.

1. Baloti grants a user the right to vote, signs his e-mail address, sends both to Selectio Helvetica
2. Selectio Helvetica sends a registration credential to the voter
3. Voter chooses his voting code and sends one share to each of the authorities A_i along with the registration credential
4. Each authority A_i maps the share of the voting code to a share of the DSA private key

Selectio Helvetica - Vote Casting

Voter makes his choice in the browser, enters his voting code and casts the vote.

1. The browser sends each authority A_i its share of the voting code
2. Each authority A_i returns its share of the mapped private key s
3. The browser reconstructs the voter's private key s (Shamir)

For instant individual verifiability, the voter shares the randomness used in the ElGamal encryption among multiple authorities.

Selectio Helvetica - Properties

Voters with a good memory

- Assuming secure platform and correct code in browser, the properties of the underlying protocol can almost be met
- The e-mail provider and the sending authority could steal a voter's registration credential, however the voter would notice

Forgetful voters

- A voter who forgets his voting code loses privacy
- He can ask the authorities to send their shares of the voting code by e-mail
- The browser can reconstruct the original voting code

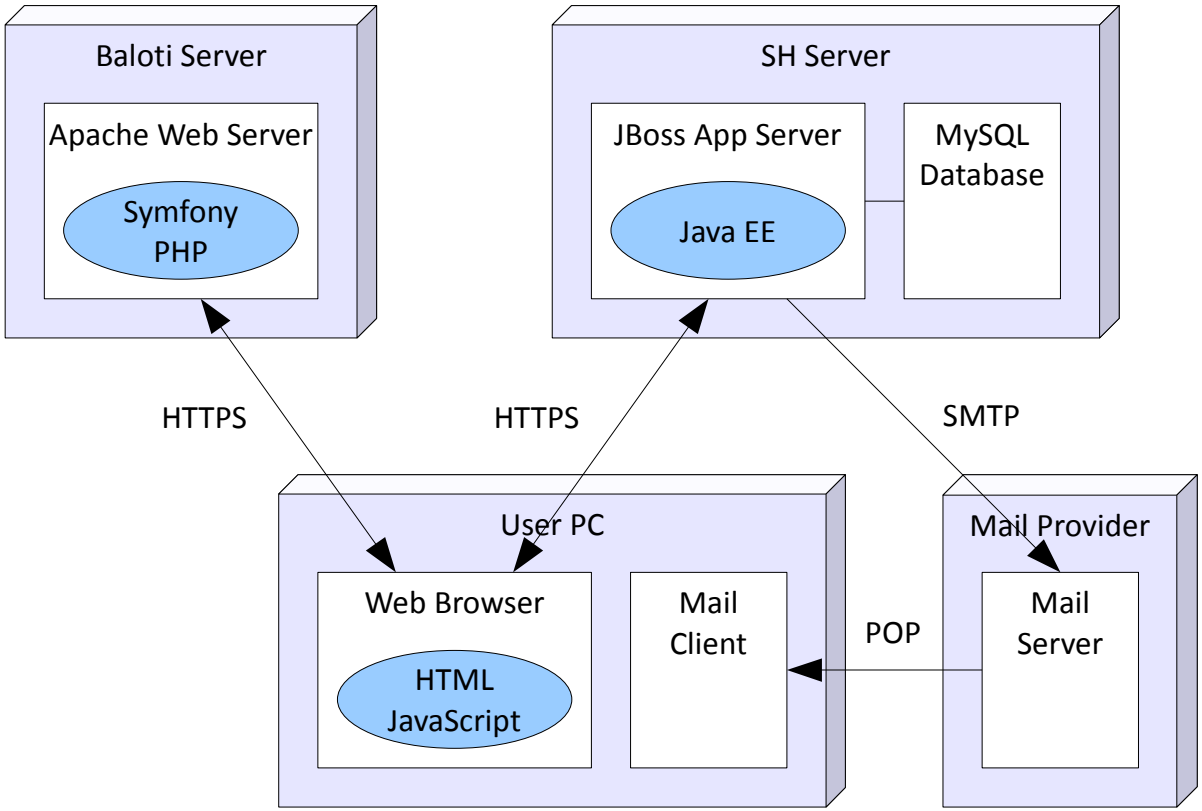
Outline

Project State

- Begin of project in spring 2010
- Realization in different stages
- First implementation (Selectio Helvetica light) is a black box
  - → only one authority (no threshold key sharing)
  - → bulletin board is not public
- Separation of concerns
  - → Baloti is responsible for the eligibility of voters
  - → SH is responsible for the e-voting process

→ Anonymity of voters towards Baloti

Architecture and Technologies



Conclusions

What we have

- Verifiable e-voting protocol
- Implementation as Selectio Helvetica light
- In operation for the referendum of September 26th, 2010

What we want

- Implementation of full Selectio Helvetica
- Project partners as trusted authorities