CYBERNETICA

On practical aspects of coercion-resistant remote voting systems

Kristjan Krips[1,3], Jan Willemson[1,2]

[1]Cybernetica
[2]STACC
[3]University of Tartu

October 4th, 2019

Motivation

- Private booth voting was introduced as a measure to guarantee voting freedom.
- However, modern technology helps breaching this privacy.
- Also, in a remote setting, there is no booth.

- Several coercion-mitigating remote voting schemes have been proposed in literature.
- This paper studies what are the explicit and implicit assumptions these schemes would need to satisfy in practice.

Schemes

We picked 7 remote voting protocols that have some coercion prevention measures:

- Estonian scheme
- NV-Civitas from the JCJ/Civitas family
- KTV-Helios from the Helios family
- BeleniosRF
- Selene
- Eos
- Selections

How to measure coercion resistance?

There are many approaches in literature. We selected the following properties:

- receipt-freeness,
- over-the-shoulder coercion resistance.

In addition, we studied whether the requirements proposed by Juels *et al.* are fulfilled:

- resistance to forced abstention,
- resistance to casting an invalid vote,
- resistance to simulation attack.

What about assumptions?

The anti-coercion properties may depend on several assumptions. We identified the following popular ones:

- special client hardware,
- anonymous channels,
- PKI / key distribution,
- subliminal password / PIN hinting with fake credentials,
- ability to cast a re-vote,
- non-trivial registration.

The Estonian scheme

- Re-voting is the only anti-coercion measure.
- Relies on special client hardware (national digital ID).
- Relies on existing PKI.

Coercion properties:

Receipt-freeness	○
Over-the-shoulder coercion resistance	●
Resistance to forced abstention	◐
Resistance to casting an invalid vote	◐
Resistance to simulation attack	◐

● = is assumed / holds ○ = is not assumed / does not hold

◐ = may hold ◑ = depends on the implementation

NV-Civitas

Relies on:

- special client hardware (smart cards + reader with trusted display),
- anonymous channels,
- PKI / key distribution,
- subliminal password/PIN hinting,
- the possibility to cast a re-vote,
- registration process that may be non-trivial.

Fulfills all of our chosen coercion properties:
receipt freeness, over-the-shoulder coercion resistance, resistance to: forced abstention / casting an invalid vote / simulation attack.

KTV-Helios

Relies on:

- special client hardware,
- anonymous channels,
- PKI / key distribution,
- the possibility to cast a re-vote.

Coercion properties:

Receipt-freeness	●
Over-the-shoulder coercion resistance	◐
Resistance to forced abstention	◐
Resistance to casting an invalid vote	◐
Resistance to simulation attack	◐

BeleniosRF

Uses:

- re-randomisable ciphertexts and signatures.

Relies on:

- PKI / key distribution.

Coercion properties:

Receipt-freeness	●
Over-the-shoulder coercion resistance	○
Resistance to forced abstention	○
Resistance to casting an invalid vote	◑
Resistance to simulation attack	○

Selene

Relies on:

- anonymous channels,
- PKI / key distribution,
- (possibility of revoting – depends on implementation).

Coercion properties:

Receipt-freeness	◐
Over-the-shoulder coercion resistance	◐
Resistance to forced abstention	◑
Resistance to casting an invalid vote	◑
Resistance to simulation attack	○

Eos

Relies on:

- special client hardware,
- anonymous channels,
- PKI / key distribution,
- subliminal password/PIN hinting,
- the possibility to cast a re-vote.

Coercion properties:

Receipt-freeness	●
Over-the-shoulder coercion resistance	●
Resistance to forced abstention	●
Resistance to casting an invalid vote	◑
Resistance to simulation attack	◑

Selections

Relies on:

- anonymous channels,
- subliminal password/PIN hinting,
- the possibility to cast a re-vote,
- a non-trivial registration process.

Coercion properties:

Receipt-freeness	◐
Over-the-shoulder coercion resistance	●
Resistance to forced abstention	◐
Resistance to casting an invalid vote	◑
Resistance to simulation attack	●

The summary of results

Table 1. Cross-table of assumptions and achieved coercion resistance properties

	Estonia	NV-Civitas	KTV-Helios	BeleniosRF	Selene	Eos	Selections
Special client hardware	●[1]	●	●	○	○	●	○
Anonymous channels	○	●	●	○	●	●	●
PKI / key distribution	●	●[2]	●	●	●[2]	●[2]	○
Subliminal password/PIN hinting	○	●	○	○	○	●	●
Casting a re-vote	●	●	●	○	◑[3]	●	●
Non-trivial registration	○	◑[4]	○	○	○	○	●
Receipt-freeness	○	●	●	●	◐[5]	●	◐[6]
Over-the-shoulder coercion resistance	●	●	◐[7]	○	◐[8]	●	●
Resistance to forced abstention	◐[9]	●	◐[10]	○	◑[11]	●	◐[12]
Resistance to casting an invalid vote	◐[9]	●	◐[13]	◑[14]	◑[15]	◑[16]	◑[17]
Resistance to simulation attack	◐[18]	●	◐[19]	○	○[20]	◑[21]	●[22]

● = is assumed / holds ○ = is not assumed / does not hold ◐ = may hold
◑ = depends on the implementation

Conclusions

- More assumptions → higher coercion resistance.
- More assumptions → higher complexity.
- Some assumptions are more realistic:
  - PKI, ability to cast a re-vote.
- Others less so:
  - anonymous channels, special client hardware, fake credentials.
- It is difficult to get detailed information about the protocols.
- Implementing proof-of-concept applications before publishing future schemes would be a big step forward.