“Electronic voting is in danger”

Sven Heiberg
Cybernetica, STACC

19.07.2012

Draft of the Election Law

- §48. Verification of the i-vote
  - (1) The voter can verify whether the vote given by internet voting has been sent to i-voting system according to the voter's intention.
  - (2) Verification procedures are established by Electoral Commission.

I-voting protocol since 2005

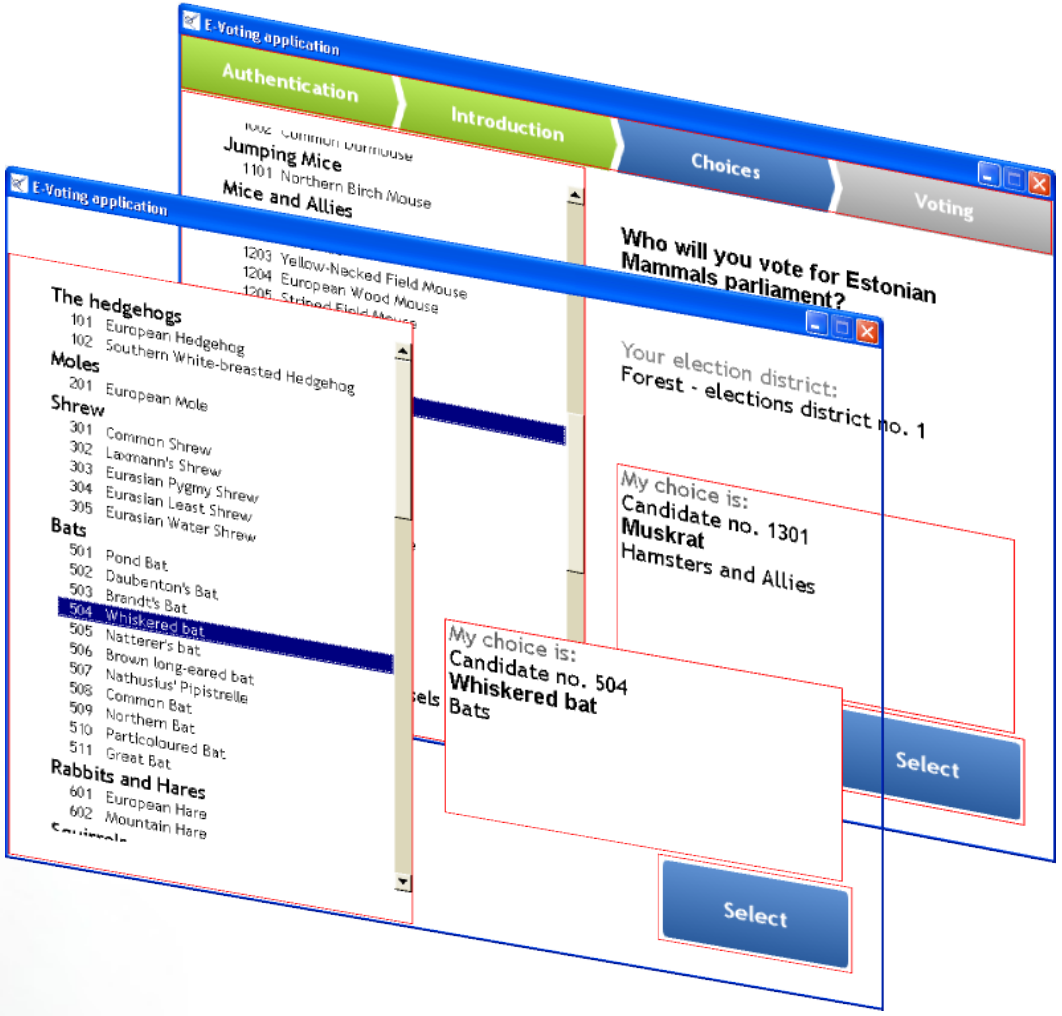
(1): ID-card authentication

(2): List of candidates

(3): $Sig_V(Enc_S(Rnd,Vote))$

- Parliamentary elections 2011
  - 24.3% of all the voters i-voted
  - Proof-of-concept malware attack
  - Very high political interest on the subject

Problems I: Manipulation



Problems II: Revocation

Vabariigi Valimiskomisjon

KAEBUS 8. märts 2011

Käesolevaga esitan kaebuse 2011. aastal Riigikogu valimisel elektrooniliselt antud häälte tühistamiseks.

Problems III: Reputation

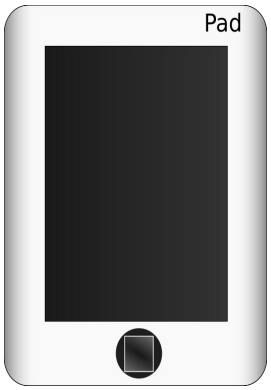
I-voting with vote auditing

(1): ID-card authentication

(2): List of candidates, OTP

(3): $Sig_V(Enc_S(Rnd,Vote))$

(4): Rnd, OTP



(5): OTP

(6): $Sig_S(Sig_V(Enc_S(Rnd,Vote)))$ List of candidates

Protocol design decisions

- Verification environment
  - Mobile vs. PC vs. kiosk
- Transport of randomness
  - Paper, USB, QR
- Verification in time
  - After the election verification – problems
- Verification algorithms
  - Brute-force vs. user input

How to apply verifiability?

- How to communicate verifiability so, that it adds to the confidence?
- How to get voters to actually verify?
  - How to get them to report errors?
- What can be done in case of an incident?
  - What to do if the situation escalates?
- How to prevent few dishonest from spoiling the party for others?

“Electronic voting is in danger”

- “Internet banking is secure, therefore e-voting can be secure”
- “Liars are real threat, not malware”
- “Verifiability is too complex – look at Norwegian problems”
- “People do not understand verifiability”
- “Secret agenda is to get rid of e-voting”
- “I have secure e-voting protocol”
- “Nobody is going to use it”

Thank you!

- Discussions