Recent Developments in Estonian i-Voting

Arnis Parovs

arnis@ut.ee

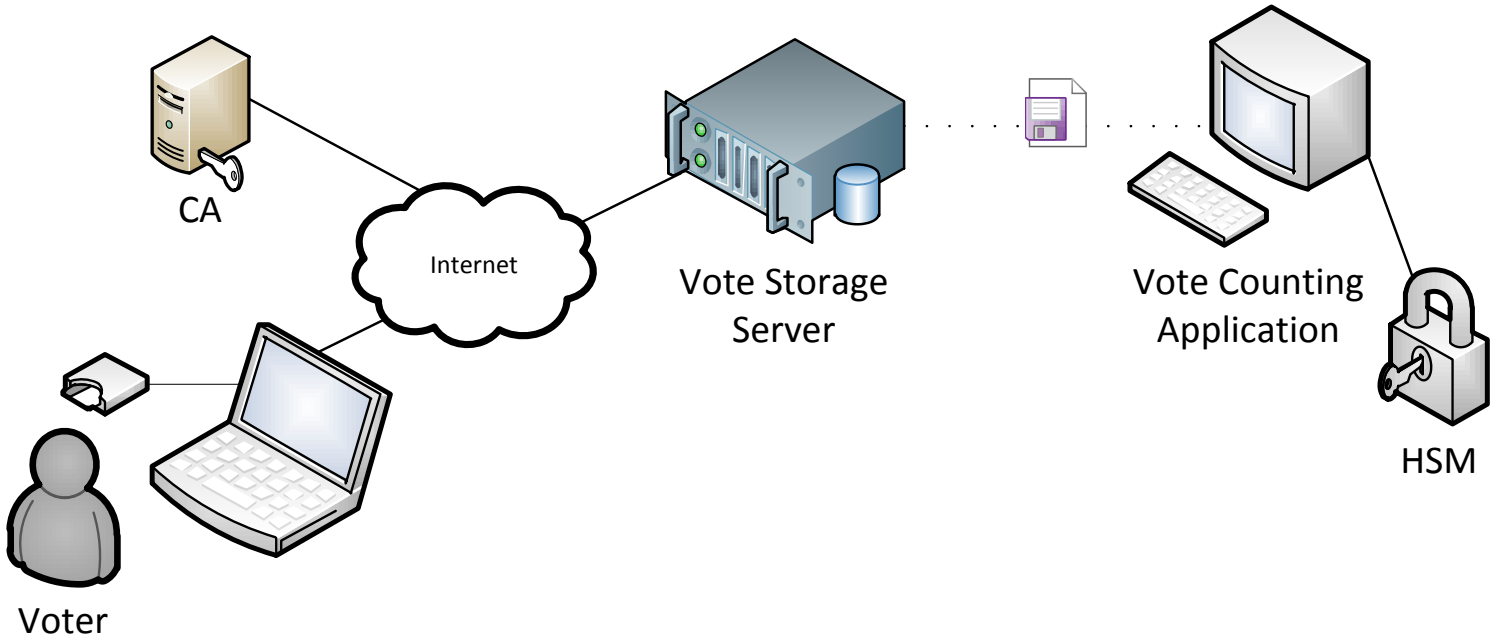
November 14, 2013

STACC Software Technology and Applications Competence Center

European Union
Regional Development Fund

Investing in your future

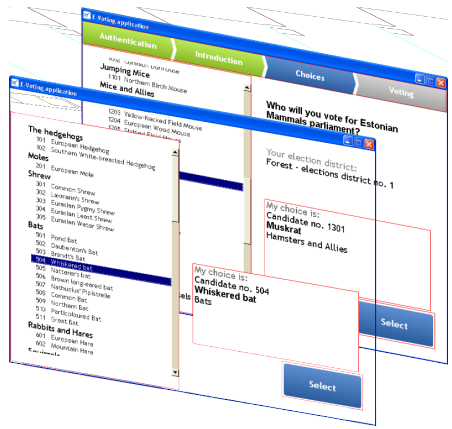
Estonian Internet Voting Scheme



$b_{anon} = Enc_{s_{pub}}(c, rnd)$ – RSA-OAEP
$b = Sig_v(b_{anon})$ – Digital Signature by Estonian ID-card

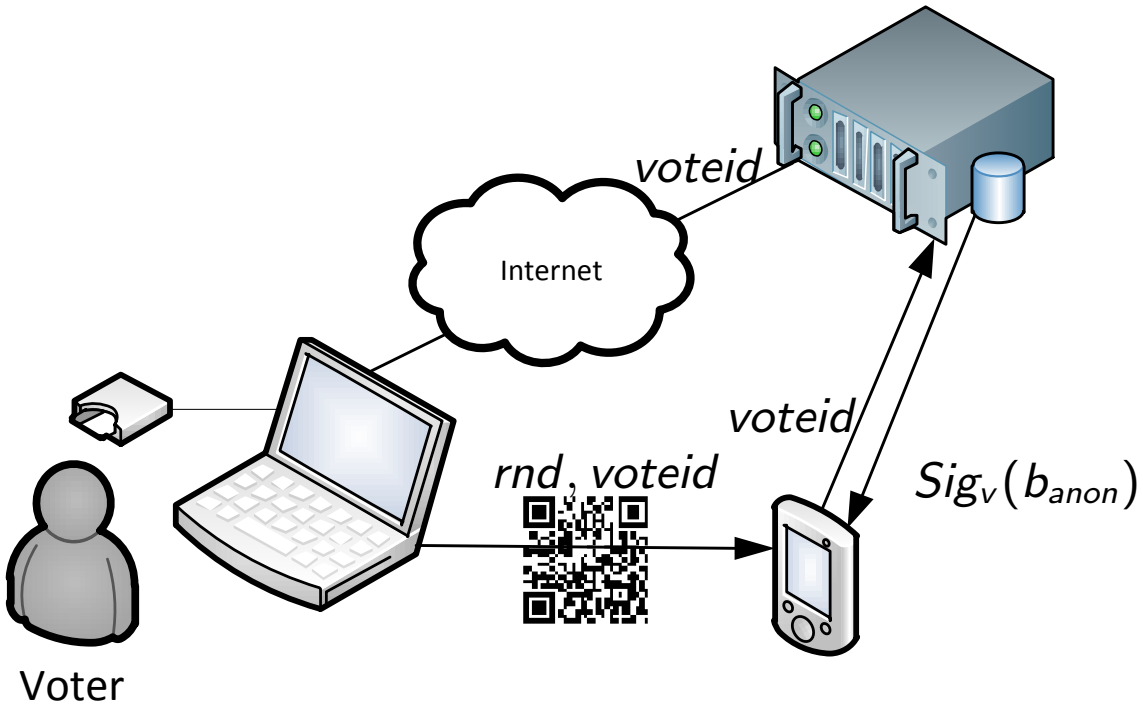
Parliamentary Elections 2011

- I-voting since 2005
- 24.3% votes cast by i-voting
- Proof-of-concept malware



- Revocation appeals
- Invalid i-vote
- Re-voting 500+ times
- Reputation attacks

Cast as Intended Verification



- Crack the vote by re-encrypting candidates
- Supports Android only (iOS and Windows planed)

Municipal Elections 2013

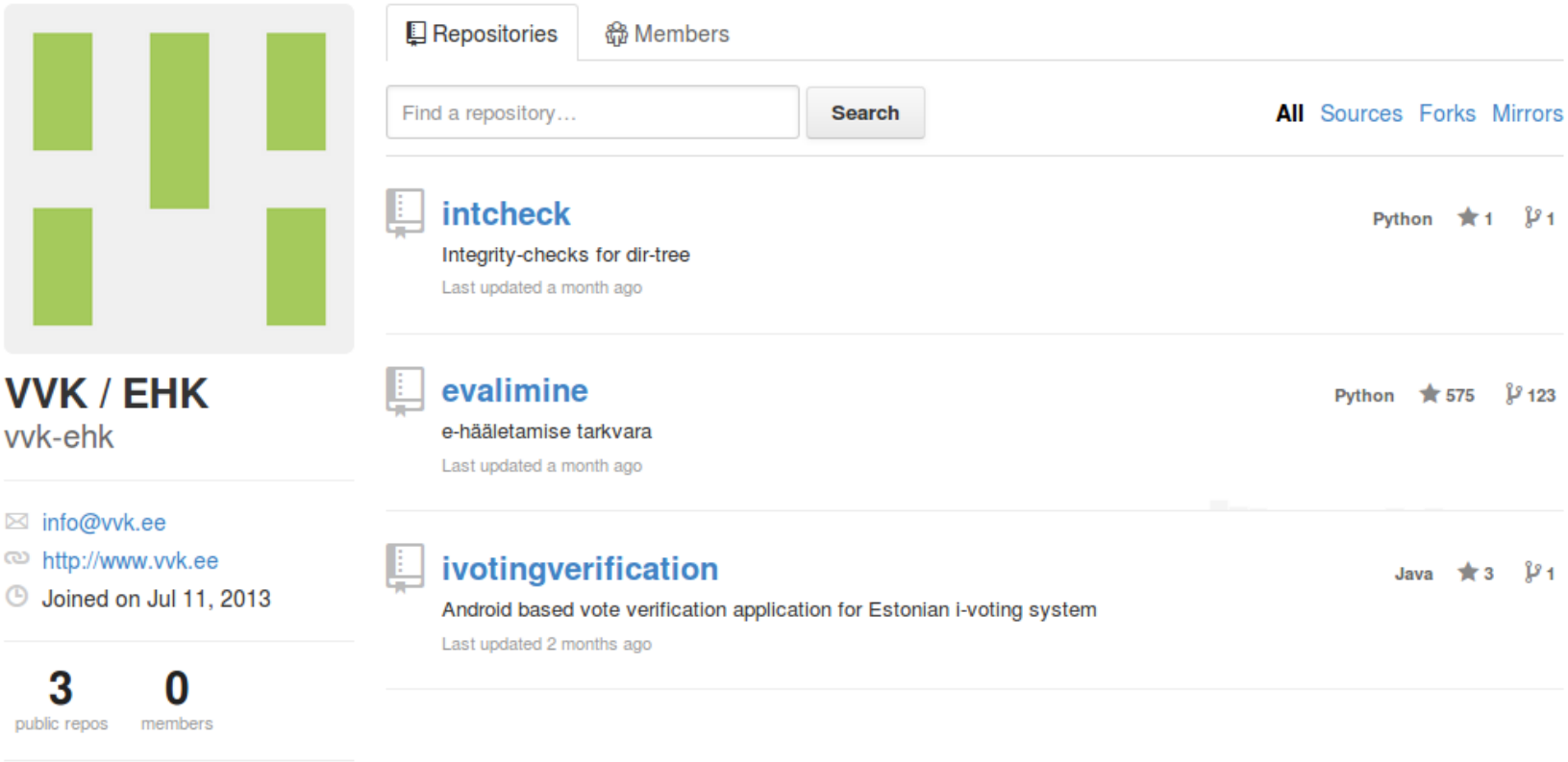
- 21.2% votes cast by i-voting
- Out of 133808 votes verified 4696 (3.43%)
  - No complaints received
- Invalid i-vote
- Reputation attacks:

> "Denigration of Estonia's e-elections has also reached record heights, with Tallinn city government advertising its forum called "Satan Votes in Internet", trying to scare people off e-elections, claiming it is insecure."
>
> `http://news.postimees.ee/2439174/editorial-unbelievable-antics-for-taxpayer-money`

- No revocation appeals
- Vote buying cases (not involving i-voting)
- European Parliament elections – May 2014

Source Code Published

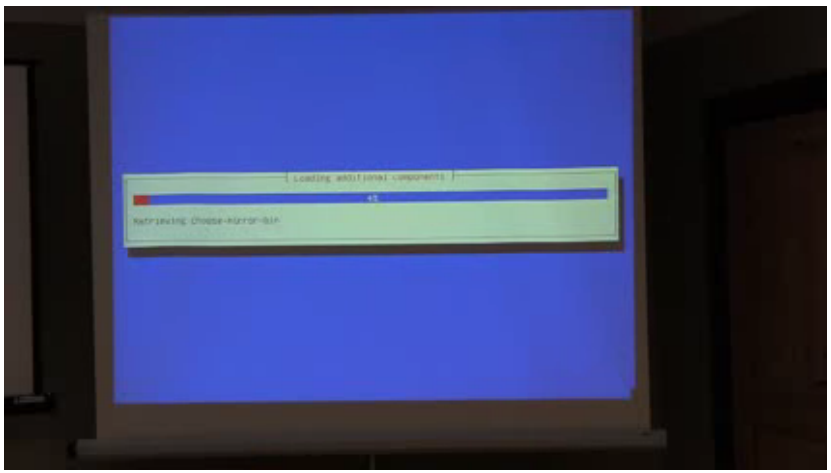
`https://github.com/vvk-ehk/`

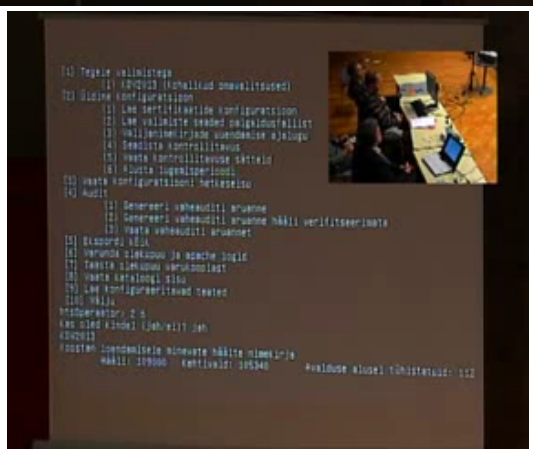


- Code comments in Estonian
- Client application code not published

Procedures Published

http://www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ





Thank you!

Questions, comments, opinions?