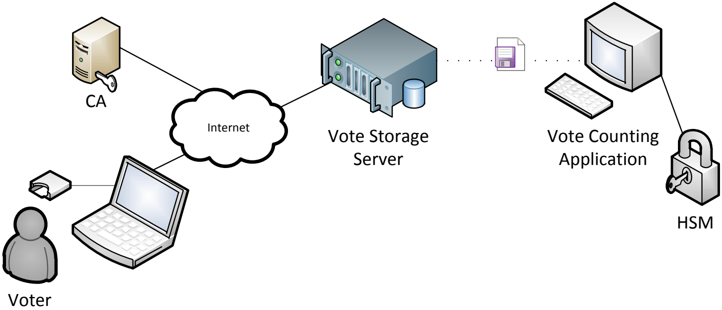
Estonian Internet Voting

Arnis Paršovs

arnis@ut.ee

October 16, 2012

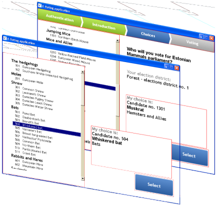
Estonian Internet Voting Scheme



$b_{anon} = Enc_{s_{pub}}(c, rnd)$ – 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



Jumping Mice
1101 Northern Birch Mouse
Mice and Allies
1203 Yellow-Necked Field Mouse
1204 European Wood Mouse

Who will you vote for Estonian Mammals parliament?

Your election district:
Forest - elections district no. 1

My choice is:
Candidate no. 1301
Muskrat
Hamsters and Allies

The hedgehogs
101 European Hedgehog
102 Southern White-breasted Hedgehog
Moles
201 European Mole
Shrew
301 Common Shrew
302 Laxmann's Shrew
303 Eurasian Pygmy Shrew
304 Eurasian Least Shrew
305 Eurasian Water Shrew
Bats
501 Pond Bat
502 Daubenton's Bat
503 Brandt's Bat
504 Whiskered bat
505 Natterer's bat
506 Brown long-eared bat
507 Nathusius' Pipistrelle
508 Common Bat
509 Northern Bat
510 Particoloured Bat
511 Great Bat
Rabbits and Hares
601 European Hare
602 Mountain Hare

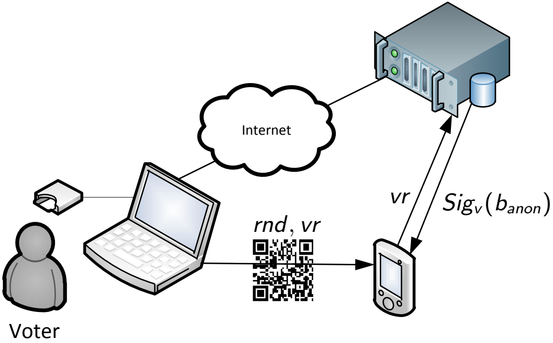
My choice is:
Candidate no. 504
Whiskered bat
Bats

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

OSCE/ODIHR Report 2011

The OSCE/ODIHR recommends that the NEC forms an inclusive working group to consider the use of a verifiable Internet voting scheme or an equally reliable mechanism for the voter to check whether or not his/her vote was changed by malicious software.

Individually Verifiable Vote Auditing Scheme



- Crack the vote by brute-forcing candidates
- Re-voting attack
- For how long *vr* should work?

Amendments in 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.

CoE Recommendations for e-voting

A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.

Coercion/Vote-buying

- Possible vectors:
    - Observe voting
    - Obtain ID-card
- Verifiability adds coercion vectors
    - QR code as receipt
- Re-voting as anti-coercion measure
    - Internet re-voting
    - Re-voting in polling station (cancels i-vote)
- Remote voting methods vulnerable
- Coercion attacks rather inefficient

What Verifiability Solves?

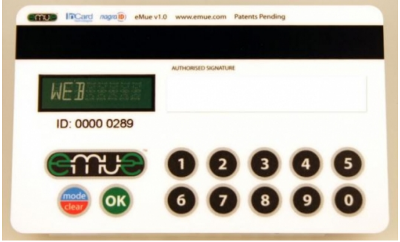
- Detection of election rigging malware
- Decrease revocation appeals?
- Improve reputation of i-voting?

Norwegian Experiences with Verifiable Electronic Voting

In addition to the 74 (out of 28,001) reports on incorrect bindings, the support call center received another 35 return code related calls:

- 11 voters reported not having received a poll card
- 5 voters **who voted online reported not receiving a return code**
- 4 voters received a poll card with the return codes smeared
- 1 person received two poll cards, one with the correct binding and one incorrect
- 2 callers reported **having received return codes without having voted**

Voting in ID-card



- Voting application in ID-card
- Preserves vote secrecy
- Protection against disenfranchisement attack
  $Enc_{s_{pub2}}(b, vcode)$
  $vcode_{sent\_encrypted} == vcode_{received\_plain}$?
- Smart card application updates
- Force ID-card to leak *rnd* for auditing

Thank you!

Questions, comments, opinions?