New technologies for democratic elections

Sven Heiberg
SBP'12
Tallinn

03.09.2012

A bit of history

• First reports on Estonian i-voting in 2001
• Following principles were developed in 2003 to suit the legal framework:
  • Principles of paper-voting are followed
  • i-voting during the advance voting period
  • The voter uses ID-card
    • System authenticates the voter
    • Voter confirms his/her choice with digital signature
I-voting protocol since 2005

1. ID-card authentication
2. List of candidates
3. $\text{Sig}_v(\text{Enc}_s(\text{Rnd}, \text{Vote}))$

I-voting in Estonia

<table>
<thead>
<tr>
<th>Year</th>
<th>% of citizens</th>
<th>% of voters</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005 Loc.Munic.</td>
<td>0</td>
<td>1.8</td>
</tr>
<tr>
<td>2007 Parliament</td>
<td>1.5</td>
<td>3.5</td>
</tr>
<tr>
<td>2009 Eur.Parliament</td>
<td>5.0</td>
<td>7.2</td>
</tr>
<tr>
<td>2011 Parliament</td>
<td>10.0</td>
<td>13.5</td>
</tr>
</tbody>
</table>
I-voting is possible!

Threats to election

- The purpose of the elections is delegating the power (formally vested into people) to a small set of representatives
- Increase influence in the society
  - Bribery
  - Coercion
  - Fraud
  - Disenfranchisement
  - ...

How to counter those threats?

- Have to maintain ballot secrecy
- Paper voting in polling stations
  - Privacy of polling-booth
  - Observation of the procedures
- Voter can i-vote from anywhere
  - Have to trust computer
  - Electronic process are not observable
  - Attacks scale

Verifiability

- Verifiability reduces trust to voting system and voting environment
- Individual verifiability – voter has means to verify some of following properties about the ballot:
  - Cast as intended
  - Accepted as cast
  - Tallied as recorded
- Universal verifiability – public means to observe correctness of tally
Individual verifiability: Norway

- Log on
- Submit vote

E-voting system

Receipt code

http://www.regjeringen.no

We do not want verifiability!
Parliamentary election 2011

- Election rigging malware developed by a student
  - Wanted public attention, attempted revocation
- Voting application defect used in political battle
- I-voting has become so significant that it makes sense to attack it

Risk-analysis

Attack strategies

Three main attack classes

Violating the requirements

Specific techniques

Generic techniques
Main attack classes

- Manipulation attacks
  - „Classical“ attacks against uniformity, correctness, freedom, etc.
- Revocation attacks
  - Referring to a real attack, try to achieve cancelling all the i-votes, hoping to change the outcome of the tally
- Reputation attacks
  - Try to discredit i-voting and hope that people who choose not to i-vote will not vote at all

We need verifiability!

- Fight against real manipulation attacks
- Discourage potential real attackers
- Prevent revocation and reputation attacks
  - This item is actually the most important one, since reputation attacks are cheap, risk-free and can be expected to have huge impact
I-voting with vote auditing

(1): ID-card authentication
(2): List of candidates, OTP
(3): $\text{Sig}_V(\text{Enc}_S(\text{Rnd}, \text{Vote}))$
(4): Rnd, OTP
(5): OTP
(6): $\text{Sig}_S(\text{Sig}_V(\text{Enc}_S(\text{Rnd}, \text{Vote})))$

Draft of the new 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.
Last but not least...

- Verifiability has to be supported by incident handling
- Verifiability changes the way voters perceive elections
  - Is ballot secrecy under doubt?
  - Does verifiability ease coercion?
  - Can verifiability be misused?
  - Do we need universal verifiability?
  - Do we need verifiability for paper voting?

Questions?