Internet Voting Technology

Sven Heiberg, sven@ivotingcentre.ee

May 16th, 2019
Elections

- §1 – Estonia is independent and sovereign democratic republic. The supreme power is vested in the people
- §56 – People exercise their **power** through citizens’ right to vote
- Electoral systems determine the means by which the votes are translated into seats
- There is a pre-programmed conflict in every election
  - Transfer 900 000 opinions into 101 seats - this is lossy compression
- Voting methods determine the means by which votes are gathered from the eligible voters
Internet voting

- Electronic voting: a voting method that relies on the help of electronic device(s) in performing any of its core functions
  - eligibility verification;
  - voting;
  - recording of the votes;
  - storing votes for tally;
  - tabulation of the voting result.

- Internet voting: a remote electronic voting relying on the Internet as a communication channel between the voter and the electronic ballot-box.
  - nonsupervised environment
  - voter’s device - PC, tablet, smartphone

- The Challenge: Human inability to observe electronic processes
Voting method in the election process
Voting method in the election process
Voting method in the election process

V1 → Vote → Store → Tab. → Voting Result

V2 → Vote → Store → Tab. → Voting Result

V3 → Vote → Store → Tab. → Voting Result

V4 → Vote → Store → Tab. → Voting Result

V5 → Vote → Store → Tab. → Voting Result

V6 → Vote → Store → Tab. → Voting Result

V7 → Vote → Store → Tab. → Voting Result

V8 → Vote → Store → Tab. → Voting Result

V9 → Vote → Store → Tab. → Voting Result
Voting method in the election process
Voting method in the election process

Observation

Vote -> Store -> Tab. -> Voting Result

V1 -> V2 -> V3

V4 -> V5

V6 -> V7

V8 -> V9

Election Result

Manipulation
Voting method in the election process

Vote → Store → Tab. → Voting Result → Election Result

V1

V2

V3

V4

V5

V6

V7

V8

V9

Observation

Manipulation

Vote → Store → Tab. → Voting Result
Voting method in the election process

The diagram illustrates the voting process with nine voters (V1 to V9). Each voter casts a vote, which is then recorded and stored. The votes are summarized (Tabulated) to determine the voting result. These results are aggregated to determine the election result. The diagram also highlights potential manipulation.
General challenges with voting methods

- Integrity of the voting result
  - Eligibility assurance
  - Vote integrity throughout the process
  - Ballot-box integrity
  - Correct tabulation

- Confidentiality
  - Ballot secrecy
  - Voting result confidentiality
  - Coercion resistance

- The Challenge: How to find the right kind of balance between integrity, transparency and confidentiality?
I-voters among participating voters: 2005 - 2019
Number of i-votes: 2005 - 2019

- 2005 Local: 10,000 votes
- 2007 Parl.: 50,000 votes
- 2009 EP: 100,000 votes
- 2009 Local: 150,000 votes
- 2011 Parl.: 200,000 votes
- 2013 Local: 250,000 votes
- 2014 EP: 10,000 verified votes
- 2015 Parl.: 50,000 verified votes
- 2017 Local: 100,000 verified votes
- 2019 Parl.: 250,000 verified votes
In 2001, two (conflicting) studies on the feasibility of i-voting

In 2002, i-voting was regulated in the Election Law with the condition that the method shall not be applied before 2005

In 2003, i-voting conception developed by inclusive process (private sector, academia, NEC)
  - i-voting is allowed during the Advance Voting Period
  - e-ID is used for authentication and digital signatures
  - Repeated i-voting is allowed to counter coercion
  - Paper-vote takes precedence over an i-vote

In 2004, public tender for development won by Cybernetica AS
Estonian citizens have access to secure and reliable digital signature system since 2000

Today compulsory for all residents (Certificates can be revoked)
  - e-mail address Forename.Surname@eesti.ee
  - Key and certificate for authentication
  - Key and certificate for digital signature (legally binding!)

Alternative eID - MobileID, since May 2007
  - PKI-capable SIM cards
  - Equal legal power with ID-card
Double Envelope Scheme
Estonian Internet voting protocol: 2005 - 2011

1. Authentication
2. Candidate list $L$
3. $\text{Sig}_v(Enc_{\text{pub}}(c_v, r))$
**Figure:** Candidate list

Who will you vote for Estonian Mammals parliament?  
Click on the name of your choice.

Your election district:  
Forest - elections district no. 1

My choice is:  
Candidate no. 504  
Whiskered bat  
Bats

**Figure:** Selection

In order to confirm your vote, click *Vote* button.  
You will be asked to enter your Mobile-ID P302 code for digital signature.

Who will you vote for Estonian Mammals parliament?  

My choice is:  
Candidate no. 504  
Whiskered bat  
Bats
Risk analysis

- “The weak point of the scheme, is the need to trust central servers and computers of the voters. Is such a compromise reasonable? In our opinion – yes.” (Ansper et al., 2003)
- Vulnerabilities exist, countermeasures also exist, residual risk is accepted
  - Cryptography - authentication, ballot secrecy, integrity
  - Security engineering - system architecture, deployment
  - Organization - documented audited procedure developed according to risk analysis
2011

E-Voting application

Authentication

Introduction

Choices

Voting

Who will you vote for Estonian Mammals parliament?

Your election district:
Forest - elections district no. 1

The hedgehogs
101. European Hedgehog
102. Southern White-breasted Hedgehog

Moles
201. European Mole

Shrew
301. Common Shrew
302. Lemann's Shrew
303. European Pygmy Shrew
304. European Least Shrew
305. European Water Shrew

Bats
501. Pend Bat
502. Daubenton's Bat
503. Barbast 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

Endgame

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

My choice is:
Candidate no. 504
Whiskered Bat

Select
Risk analysis revisited

- Peak in turnout - over 24 % of i-votes
- Student develops proof-of-concept vote manipulating malware and attempts revocation of voting result
- i-voting has become significant enough to attack it
- It was agreed in 2011 - we need verifiability on the client side
  - Fight against real large-scale manipulation attacks
  - Prevent revocation and reputation attacks
Verifiability

How can you trust a voting machine or electronic tabulation?
Individual verifiability

- Voter has means to verify some of following claims
  - Voting tool correctly encoded my will as a vote (*cast as intended*)
  - My vote was accepted into ballot-box (*recorded as cast*)
  - My vote was tabulated correctly (tabulated as recorded)
- How are verifiability and coercion related?
Universal verifiability

- Observer has means to directly verify following claims
  - Only votes by eligible voters are in ballot-box
  - At most one vote per voter is in ballot-box
  - No un-authorized modifications to ballot-box have occurred
  - The result is calculated correctly

- How are verifiability and ballot secrecy related?
1. Authentication

2. Candidate list $L$

3. $\text{Sig}_V(\text{Enc}_{\text{pub}}(c_v, r))$

4. Vote reference $vr$

5. $r, vr$

6. $vr, \text{Enc}_{\text{pub}}(c_v, r), L$

7. $\text{Enc}_{\text{pub}}(c_v, r), L$

Estonian Internet voting protocol 2013 - 2015
Individual verifiability detection rates

The diagram illustrates the probability of detection (%) against the amount of votes influenced by client-side manipulation. It shows different curves for various years:

- 2013 Local, 3.4%
- 2015 Parl., 4.3%
- 2019 Parl., 5.3%

The x-axis represents the amount of votes influenced, while the y-axis represents the probability of detection.
The trustworthiness of the system and its operations?

2003: "The other side of the compromise or, in principle, the weak point of the scheme, is the need to trust central servers and computers of the voters. Is such a compromise reasonable? In our opinion – yes."
The trustworthiness of the system and its operations?

- 2013: ”The other side of the compromise or, in principle, the weak point of the scheme, is the need to trust central servers and computers of the voters. Is such a compromise reasonable? In our opinion—yes.”

- Number of physical and organizational measures to ensure the trustworthiness...
  - ...that can always be cast under the shadow of a doubt.
  - The application of these measures requires high technical level of involvement of the NEC.

- How can we really prove to a third party that the voting result is correct according to the rules?
Shortcomings: tabulation integrity

- It is not possible to verify the correctness of the decryption.
- Compromised tabulation tool could change the result without anyone noticing.

\[
\text{3. } \text{Sig}_v(\text{Enc}_{\text{pub}}(c_v, r)) \quad \text{Enc}_{\text{pub}}(c_1, r_1) \quad \text{Enc}_{\text{pub}}(c_n, r_n) \quad z_1, \ldots, z_n
\]
Shortcomings: i-ballot box integrity

- Assuming the outer envelope (a.k.a. signature) can not be forged, ballot box stuffing and vote manipulation are practically unachievable.

- However, a malicious ballot box may choose to drop votes.
Third party auditability

- We want to allow a third party auditor\(^1\) to verify i-ballot box properties in a privacy preserving manner.
  - The auditor should be able to check the eligibility, well-formedness and tallied-as-recorded properties.
  - We need assurance that there is no invisible way to drop votes.
- If the integrity of the vote collection can be audited, it becomes possible to outsource this procedure.
- The verifiability of the correct tabulation would increase the trustworthiness of the voting result.

\(^1\)In principle, Anyone. In practice, limitations may apply.
Vote Collector shall register each vote to an independently hosted Registration Service.

The consistency shall be audited both by voters and auditors.
The tabulation application shall provide a proof of correct decryption for each ballot.
The i-ballot box processor audits the vote collection and anonymizes votes for the tabulation.
In order to provide an external auditor with access to both digitally signed votes and decryption proofs, a verifiable re-encryption mix-net must be applied.
IVXV: Complete audit of an election

- Data Auditor would have to audit
  - All votes in $D_{VC}$ belong to eligible voters and verify successfully,
  - All votes are consistent with the rules of well-formedness,
  - All confirmations in $D_{RS}$ verify successfully,
  - The views $D_{VC}$ and $D_{RS}$ are consistent,
  - The set of encrypted votes $B_1$ is calculated correctly,
  - $P_{mix}$ is correct,
  - $P_{dec}$ is correct,
  - $result$ is correct.
Future work / open problems

► Online voting protocols secure in the world with quantum computing
► Distributed deployments of online voting systems
► Integrity vs. privacy guarantees in the foreseeable future
► Need for external/independent auditors
Thank you!

Please read "E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005–2015)" on social studies about i-voting.