Internet Voting Technology

Sven Heiberg, sven@ivotingcentre.ee

April 29th, 2021
Part I: Remote Electronic Voting over the Internet
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
Election process

- Election as a process can be divided into 4 stages
  - Preparation, Voting, Tabulation, Finalization
- There are 4 major roles in the process
  - **Voter** has a right to vote and to appeal
  - **Candidate** has a right to be elected and to appeal
  - **Election official** has a right to revoke a single vote or the election result. Has a duty to determine the election result
  - **Observer** has a right to observe procedures of election officials during all stages of the process and to notify election officials in case of problems
Voting methods

- Voting methods are there to support electoral systems – by voting methods ballots are gathered
- There should be enough voting methods to ensure that every citizen has access to elections in a way as it is stated in the Constitution
- Voting methods are active in Preparation, Voting and Tabulation stages
Voting method in stages

- **Preparation**
  - Election officials prepare voting technology and procedures
  - Election officials prepare list of candidates and eligible voters
  - Election officials publish all relevant information to general public
Voting method in stages

- **Preparation**
  - Election officials prepare voting technology and procedures
  - Election officials prepare list of candidates and eligible voters
  - Election officials publish all relevant information to general public

- **Voting**
  - Voter uses a voting tool to cast his will as a vote
  - Vote is transported to election officials by some method
  - Election official accepts the vote to ballot box
  - Election officials store the vote in the ballot box all through the voting period
Voting method in stages

- **Preparation**
  - Election officials prepare voting technology and procedures
  - Election officials prepare list of candidates and eligible voters
  - Election officials publish all relevant information to general public

- **Voting**
  - Voter uses a voting tool to cast his will as a vote
  - Vote is transported to election officials by some method
  - Election official accepts the vote to ballot box
  - Election officials store the vote in the ballot box all through the voting period

- **Tabulation**
  - Election officials open ballot box and use tabulation tool to determine the tabulation result
Voting method in stages

- **Preparation**
  - Election officials prepare voting technology and procedures
  - Election officials prepare list of candidates and eligible voters
  - Election officials publish all relevant information to general public

- **Voting**
  - Voter uses a voting tool to cast his will as a vote
  - Vote is transported to election officials by some method
  - Election official accepts the vote to ballot box
  - Election officials store the vote in the ballot box all through the voting period

- **Tabulation**
  - Election officials open ballot box and use tabulation tool to determine the tabulation result

- **In all the stages Observers can observe the procedures of election officials**
Voting method in the election process
Voting method in the election process
Voting method in the election process
Voting method in the election process

V1
V2
V3
V4
V5
V6
V7
V8
V9

Vote → Store → Tab. → Voting Result

Observation

Election Result

Vote → Store → Tab. → Voting Result

Vote → Store → Tab. → Voting Result

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

Observation

Vote  Store  Tab.

V1  V2  V3  V4  V5  V6  V7  V8  V9

Election Result

Voting Result

Manipulation
Voting method in the election process

Observation

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

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

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

Manipulation
Voting method in the election process

Observation

Vote → Store → Tab. → Voting Result

Election Result

Vote → Store → Tab. → Voting Result

Vote → Store → Tab. → Voting Result

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?
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
Part II: Internet Voting in Estonia
I-voters among participating voters: 2005 - 2019
Number of i-votes: 2005 - 2019
Estonian Internet voting: the beginning

- 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
Access to secure and reliable digital signature system since 2000

Compulsory for all residents (opt-out)
  - e-mail address Forename.Surname@eesti.ee
  - Key and certificate for authentication
  - Key and certificate for digital signature (legally binding!)

Alternative eID
  - SIM-card based Mobile-ID, since 2007
  - App-based Smart-ID, since 2017

Constant (r)evolution of the e-ID technology
Double Envelope Scheme
Estonian Internet voting protocol: 2005 - 2011

1. Authentication

2. Candidate list \( L \)

3. \( \text{Sig}_v(\text{Enc}_{c_{pub}}(c_v, r)) \)
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

Figure: Selection

In order to confirm your vote, click "Vote" button.
You will be asked to enter your Mobile-ID P002 code for digital signature.

Who will you vote for Estonian Mammals parliament?

My choice is:
Candidate no. 504
Whiskered bat
Bats
“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
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

My choice is:
Candidate no. 594
Whiskered bat
Bats

The hedgehogs
101 European Hedgehog
102 Southern White-breasted Hedgehog

Moles
201 European Moles

Shrews
301 Common Shrew
302 Long-tailed Shrew
303 Eurasian Pygmy Shrew
304 Eurasian Least Shrew
305 Eurasian Water Shrew

Bats
501 Rasp Bat
502 Desert-bats Bat
503 Blunder Bat

Wishing Bat
504 Whistler's Bat
505 Brown long-eared bat
506 Northern bat
507 Common Bat
508 Northern Bat
510 Partially Bats
511 Great Bat

Rabbits and Hares
601 European Hare
602 Mountain Hare
603 Whiskered Hare

End application
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 unauthorized modifications to ballot-box have occurred
  - The result is calculated correctly

- How are verifiability and ballot secrecy related?
Estonian Internet voting protocol 2013 - 2015

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. $vr, L$
7. $\text{Enc}_{\text{pub}}(c_v, r), L$
8. $c_v$
Individual verifiability detection rates

![Graph showing individual verifiability detection rates. The x-axis represents the amount of votes influenced by client side manipulation, ranging from 0 to 140. The y-axis represents the probability of detection, ranging from 0 to 100. The graph includes four curves, each representing different years: 2013 Local (3.4%), 2015 Parl. (4.3%), 2019 Parl. (5.3%), and a fifth line that is not labeled.]
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?
Estonian system so far

1. Authentication
2. Candidate list $L$
3. $\text{Sig}_v(\text{Enc}_{pub}(c_v, r))$
4. Vote reference $vr$
5. $r, vr$
6. $vr$
7. $\text{Enc}_{pub}(c_v, r), L$
8. $c_v$

$\text{OCSP}$

$\text{VFS/VSS}$

$\text{TA/HSM}$

$c_1, \ldots, c_n$
Shortcomings: tabulation integrity

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

\[ 3. \, \text{Sig}_v(\text{Enc}_{\text{pub}}(c_v, r)) \]
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
- Browser-based and/or mobile voting
- Biometric identity validation
Thank you!

- Please read "E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005–2015)" on social studies about i-voting.
- Please read "On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards"
- Please read "Introducing TIVILEDGE: Next Generation Blockchain Online Voting"