Internet Voting Technology

Sven Heiberg, sven@ivotingcentre.ee

April 20th, 2017
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

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

- Observers can observe the procedures of election officials
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

V1
\[ V2 \]
\[ V3 \]
\[ V4 \]
\[ V5 \]
\[ V6 \]
\[ V7 \]
\[ V8 \]
\[ V9 \]
Voting method in the election process

V1 \rightarrow Vote \rightarrow Store \rightarrow Tab. \rightarrow Voting Result

V2 \rightarrow Vote \rightarrow Store \rightarrow Tab. \rightarrow Voting Result

V3

V4

V5 \rightarrow Vote \rightarrow Store \rightarrow Tab. \rightarrow Voting Result

V6

V7 \rightarrow Vote \rightarrow Store \rightarrow Tab. \rightarrow Voting Result

V8

V9

Observation

Election Result
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

Observation

V1
V2
V3
V4
V5
V6
V7
V8
V9

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
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
Estonian Internet voting: the beginning

- In 2001, two studies on the feasibility of i-voting in 2002
  - Ministry of Justice: it is unrealistic to implement statewide i-voting in 2002 (Lipmaa et al., 2001)
  - Ministry of Transport and Communications: it is possible to implement statewide i-voting in 2002 (Tammet et al., 2001)
- 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!)
- RSA2048 since 2011, RSA1024 on earlier cards
- Pinpad readers promoted to tackle the biggest vulnerability

Alternative eID - MobileID, since May 2007
- PKI-capable SIM cards
- Equal legal power with ID-card
- ECC starting from 2015
Double Envelope Scheme
Estonian Internet voting protocol: 2005 - 2011

1. Authentication

2. Candidate list $L$

3. $\text{Sig}_v(\text{Enc}_{s_{pub}}(c_v, r))$
The application allows voters to select candidates for the Estonian Mammals parliament. The candidate list includes various mammal species, such as bats, hedgehogs, and squirrels. The selection process involves choosing a candidate number. The interface includes buttons for canceling or selecting a candidate and a button for finalizing the vote.
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
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. 504
Whiskered bat
Bats
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)
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
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. $vr$

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

8. $c_v$
Estonian Internet voting protocol 2013 - 2015

- Introducing verifiability required changes in the Election Law
  - Lot of consultations with the stakeholders
  - Agreed on the *cast as intended* and *recorded as cast*
- Non-binding pilots in 2013 Local and 2014 EP elections
  - Fully in effect in 2015 Parliamentary elections
Verification in 2013 - 2015

![Graph showing probability of detection against amount of votes influenced for different years: detectrate2013(x, 4696), detectrate2014(x, 4207), detectrate2015(x, 7787).]
Estonian system so far

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

OCSP

VFS/VSS

TA/HSM

$\text{Enc}_{\text{pub}}(c_1, r_1)$

$c_1, \ldots, c_n$

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

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.

\[ \text{Sig}_v(\text{Enc}_{\text{pub}}(c_v, r)) \]

3. Vote reference \( vr \)

4. \( \text{Enc}_{\text{pub}}(c_1, r_1) \)

5. \( r, vr \)

6. \( vr \)

7. \( \text{Enc}_{\text{pub}}(c_v, r), L \)
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.
Conclusions and further work

- The Estonian Internet voting scheme will be getting two major updates:
  - Vote Collector needs to commit the vote operations to a registration service, hence making all of its actions independently auditable;
  - The tabulation application will issue proofs of correct decryption.
    - To allow full independent auditability, a mix-net needs to be applied.
- The first update is scheduled to be implemented by fall 2017 local elections; we sincerely hope that it is possible to implement the second update by that time, too.
Part III: Performance Requirements for End-to-End Verifiable Elections
Verifiability

- The term verifiability emerged with electronic voting methods
- How can you trust a voting machine or electronic tabulation?
- Verifiability reduces trust to voting system and voting environment
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)
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
End-to-end verifiability

- We suggest general performance requirements for end-to-end verifiable elections, focusing on end-to-end verifiable elections and not on voting systems: we care if the election outcome accurately reflects the intentions of the voters, regardless of whether the voting equipment is “correct” or not. That is, it is ultimately the election that is checked, not just the equipment. (Popoveniuc et. al.)
Verifiability in terms of irregularities

- Presented ballots are well-formed
- Cast ballots are well-formed
- Recorded as cast
- Tallied as recorded
- Consistency
- Each recorded ballot is subject to the recorded as cast check
Representation

- Irregularity checked
- When the check can be made
- Who may check
- What is checked
- Detection probability
- Proof, if system fails check
Presented ballots are well-formed

- If the ballot to be cast by Vivian is not well-formed, then
- When: at any time after the election
- Who: Vivian
- What: is able to detect if the vote she is about to cast does not represent a vote for the candidate(s) she intended.
- This check ensures that the ballot is interpreted in the same way by Vivian and by the voting system
Cast ballots are well-formed

- If a cast ballot $B$ (any cast ballot) is not well-formed (contains over-votes or negative votes), and is marked to be included in the tally, then
- When: at any time after the election
- Who: Ann
- What: is able to detect that the cast ballot $B$ is incorrectly formed.
- This check ensures that Vivian’s vote has the correct impact on the final tally
Recorded as cast

- Assuming Vivian’s cast ballot has been incorrectly recorded, then
- When: at any time after the election
- Who: Vivian
- What: is able to detect that her cast ballot is incorrectly recorded
- This check ensures that Vivian’s vote is recorded by the election system correctly
Tallied as recorded

▶ If $n$ recorded ballots have been incorrectly tallied, then
▶ When: at any time after the final tally has been made public by the election officials
▶ Who: Ann
▶ What: is able to detect that the declared tally does not represent the tally of all the recorded votes
▶ This requirement allows everyone to check that the announced tally has been constructed from all the recorded ballots.
Assuming that the set of recorded ballots from Tallied as recorded is not the same as the set of ballots Vivian is able to check in Recorded as cast, then

- **When:** at any time after the tally has been made public by the election officials
- **Who:** Ann
- **What:** is able to detect that the two sets are different.
Each recorded ballot is subject to the recorded as cast check

- If a cast ballot $B$ (any cast ballot) does not have a unique voter who is able to check it during the “recorded as cast” phase, then
- When: at any time after the election
- Who: Ann
- What: is able to detect that the cast ballot $B$ does not have a unique corresponding voter
Limits of the approach

- These requirements consider only for election integrity
- Out of scope
  - Voter privacy
  - Resistance to coercion and vote buying
  - Reliability
  - Usability
  - Accessibility
  - Resistance to denial-of-service attacks
- It would be rather easy to have an end-to-end voting system in which it is public how everyone voted.
Thank you!