Log Analysis of Estonian Internet Voting 2013–2015

Sven Heiberg\textsuperscript{1}  Arnis Parsovs\textsuperscript{2,3}  Jan Willemsen\textsuperscript{2,4}

\textsuperscript{1}Smartmatic-Cybernetica Centre of Excellence for Internet Voting
\textsuperscript{2}Software Technology and Applications Competence Centre
\textsuperscript{3}University of Tartu, Institute of Computer Science
\textsuperscript{4}Cybernetica

November 5, 2015
Research objective

Analyse information available to NEC in order to:

▶ Detect attacks against i-voting
▶ Detect system malfunction
▶ Study voter behaviour

Data sources:

▶ Log files produced by i-voting servers
▶ Support requests handled by NEC
▶ Public information
Estonia has i-voted since 2005

Objects of this study:
- Municipal Elections 2013 (KOV2013)
- Riigikogu Elections 2015 (RK2015)
Voting protocol in 2015

There are three sub-protocols:
- Voting with smart card-based eID
- Voting with Mobile-ID
- Vote verification with the mobile device
Logs generated on candidate list retrieval

Log analysis is not a trivial task

- Logs in KOV2013 – more than 4’000’000 loglines, 700MB
Log monitor

- Centralized logserver using rsyslog
- Log-processor
  - Parse entry, extract information, fill database
- Analysis front-end
  - Provide descriptive statistics and pattern analysis
- Pseudonymization of logs for later research
What should we look for in the data?

Normality profile:

- Describe in detail “normal” i-voting:
  - The voting session creates only expected log entries
  - The voting session ends with a successfully cast vote
  - The verification session ends with a successfully verified vote
  - The voting session is completed in a few minutes
  - Not too many voters share the same voting IP address
  - Not too many verifiers share the same verifying IP
  - The overall percentage of revoters is small
  - The vote is verified from a single IP address
  - etc.

- In total 24 features

- Anomaly pattern – inverse of normality
## Session breakdown

<table>
<thead>
<tr>
<th>Session kind</th>
<th>Kov2013</th>
<th>Ep2014</th>
<th>Rk2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>All sessions</td>
<td>176,144</td>
<td>120,503</td>
<td>211,215</td>
</tr>
<tr>
<td>Voting</td>
<td>170,801</td>
<td>114,792</td>
<td>201,811</td>
</tr>
<tr>
<td>Successful</td>
<td>80.1%</td>
<td>91.6%</td>
<td>89.7%</td>
</tr>
<tr>
<td>ID card</td>
<td>91.4%</td>
<td>89.0%</td>
<td>87.8%</td>
</tr>
<tr>
<td>Mobile-ID</td>
<td>8.6%</td>
<td>11.0%</td>
<td>12.2%</td>
</tr>
<tr>
<td>Unsuccessful</td>
<td>19.9%</td>
<td>8.4%</td>
<td>10.3%</td>
</tr>
<tr>
<td>ID card</td>
<td>76.9%</td>
<td>64.9%</td>
<td>69.1%</td>
</tr>
<tr>
<td>Mobile-ID</td>
<td>23.1%</td>
<td>35.1%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Verification</td>
<td>5,343</td>
<td>5,711</td>
<td>9,404</td>
</tr>
<tr>
<td>Successful</td>
<td>94.0%</td>
<td>85.7%</td>
<td>89.7%</td>
</tr>
<tr>
<td>Unsuccessful</td>
<td>6.0%</td>
<td>14.3%</td>
<td>10.3%</td>
</tr>
</tbody>
</table>
Unsuccessful voting sessions

<table>
<thead>
<tr>
<th>Type</th>
<th>Unsuccessful %</th>
<th>Successful %</th>
</tr>
</thead>
<tbody>
<tr>
<td>KOV2013</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>EP2014</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>RK2015</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>KOV2013</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>EP2014</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>RK2015</td>
<td>10</td>
<td>90</td>
</tr>
</tbody>
</table>
## Unsuccessful voting sessions – explicit errors

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit error</td>
<td>8,979</td>
<td>4,032</td>
<td>5,513</td>
</tr>
<tr>
<td>Common error</td>
<td>1,103</td>
<td>369</td>
<td>1,509</td>
</tr>
<tr>
<td>Maintenance</td>
<td>11</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Under-aged voter</td>
<td>28</td>
<td>16</td>
<td>30</td>
</tr>
<tr>
<td>Ineligible voter</td>
<td>1,063</td>
<td>315</td>
<td>507</td>
</tr>
<tr>
<td>Voting ended</td>
<td>1</td>
<td>38</td>
<td>89</td>
</tr>
<tr>
<td>Session expired</td>
<td>–</td>
<td>–</td>
<td>882</td>
</tr>
<tr>
<td>Certificate issue</td>
<td>1,978</td>
<td>302</td>
<td>641</td>
</tr>
<tr>
<td>Pre-2011 Mobile-ID user</td>
<td>1,490</td>
<td>549</td>
<td>366</td>
</tr>
<tr>
<td>Bad Mobile-ID number</td>
<td>2,051</td>
<td>491</td>
<td>974</td>
</tr>
<tr>
<td>DigiDocService failure</td>
<td>47</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mobile-ID failures</td>
<td>2,217</td>
<td>1,148</td>
<td>1,956</td>
</tr>
<tr>
<td>Incident</td>
<td>93</td>
<td>1,173</td>
<td>67</td>
</tr>
</tbody>
</table>
Unexpected log entries – incidents

▶ KOV2013
▶ 37 failed ID card sessions – buggy OpenSC
▶ 36 failed voting sessions – problematic backup routine
▶ 17 malformed votes – lack of error checking in voting client
▶ 3 invalid cell numbers – lack of input validation in voting client

▶ EP2014
▶ 1131 failed voting sessions – timezone bug in cert verification
▶ 42 incidents with buggy OpenSC or failed M-ID
▶ 196 malformed vote verification requests – iOS verification application
▶ 5 ID card sessions with card switching
▶ 6 sessions with incorrect session state change

▶ RK2015
▶ 1 failed session – inaccessible voter list
▶ 2 ID card sessions with card switching
▶ 4 ID card sessions vote signature invalid
▶ 1 ID card session with invalid certificate signature
▶ 59 Mobile-ID sessions using outdated voting client
▶ 615 verification sessions using outdated verification application
▶ 19 sessions with incorrect session state change
Other reasons for failure

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>Voters</td>
<td>Sessions</td>
<td>Voters</td>
</tr>
<tr>
<td>Other reason</td>
<td>24,969</td>
<td>16,087</td>
<td>5,593</td>
</tr>
<tr>
<td>Discontinued (Mobile-ID)</td>
<td>826</td>
<td>595</td>
<td>672</td>
</tr>
<tr>
<td>Authentication</td>
<td>636</td>
<td>470</td>
<td>461</td>
</tr>
<tr>
<td>Signing</td>
<td>190</td>
<td>178</td>
<td>211</td>
</tr>
<tr>
<td>Abnormal</td>
<td>40</td>
<td>34</td>
<td>0</td>
</tr>
<tr>
<td>Vote not submitted</td>
<td>24,103</td>
<td>15,563</td>
<td>4,921</td>
</tr>
<tr>
<td>ID card</td>
<td>23,004</td>
<td>14,630</td>
<td>4,524</td>
</tr>
<tr>
<td>Mobile-ID</td>
<td>1,099</td>
<td>954</td>
<td>397</td>
</tr>
</tbody>
</table>
Unsuccessful voting sessions – failure to cast a vote

- Abandoned voting sessions – candidate list is successfully downloaded, but the vote is never cast
- Forgotten PIN to access the signing key
- Bugs in voting client (KOV2013)
- Probably not disenfranchisement attack – would be noticed by verification

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Voters</th>
<th>Voters (u)</th>
<th>Sessions</th>
<th>Voters</th>
<th>Voters (u)</th>
<th>Sessions</th>
<th>Voters</th>
<th>Voters (u)</th>
</tr>
</thead>
</table>
## Verification errors

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsuccessful sessions</td>
<td>319</td>
<td>84</td>
<td>787</td>
<td>106</td>
<td>965</td>
<td>218</td>
</tr>
<tr>
<td>Newer vote cast</td>
<td>19</td>
<td>6</td>
<td>11</td>
<td>6</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>Verification count exceeded</td>
<td>144</td>
<td>47</td>
<td>317</td>
<td>81</td>
<td>154</td>
<td>63</td>
</tr>
<tr>
<td>Verification time exceeded</td>
<td>95</td>
<td>54</td>
<td>78</td>
<td>39</td>
<td>121</td>
<td>63</td>
</tr>
<tr>
<td>Vote ID not issued</td>
<td>60</td>
<td>–</td>
<td>185</td>
<td>–</td>
<td>58</td>
<td>–</td>
</tr>
<tr>
<td>Abnormal state</td>
<td>1</td>
<td>1</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Malformed vote ID</td>
<td>–</td>
<td>–</td>
<td>196</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Invalid verification request</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>615</td>
<td>104</td>
</tr>
</tbody>
</table>
## Support requests

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>QR code focusing problems</td>
<td>8</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>State-revoked ID cards (issued in 2011)</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Android VVA crash</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Outdated ID-software, drivers</td>
<td>9</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>IVCA Internet connectivity issues</td>
<td>109</td>
<td>24</td>
<td>0</td>
</tr>
<tr>
<td>Unsupported voting platforms</td>
<td>3</td>
<td>0</td>
<td>101</td>
</tr>
<tr>
<td>Pre-2011 Mobile-ID user</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>PIN code issues</td>
<td>3</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>ID-software not installed</td>
<td>13</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IVCA errors 0xX</td>
<td>13</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MacOS X without ID-software</td>
<td>0</td>
<td>41</td>
<td>0</td>
</tr>
<tr>
<td>Website related</td>
<td>0</td>
<td>14</td>
<td>12</td>
</tr>
<tr>
<td>Certificates not yet valid bug</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>iOS-based VVA 0-byte bug</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>ID-card certificates expired</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>General election questions</td>
<td>0</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td>Built-in card readers, drivers</td>
<td>0</td>
<td>0</td>
<td>75</td>
</tr>
<tr>
<td>Other</td>
<td>85</td>
<td>49</td>
<td>109</td>
</tr>
</tbody>
</table>
IP address shared by several voters

On average one IP shared by:

- KOV2013: 1.95 voters
- EP2014: 1.97 voters
- RK2015: 2.11 voters

IP addresses shared by more than 100 voters:

- KOV2013: 28 IPs (top IP shared by 1,127 voters)
- EP2014: 22 IPs (top IP shared by 970 voters)
- RK2015: 28 IPs (top IP shared by 1,415 voters)
IP address shared by several voters

- Activity not evenly distributed over the voting period
  - short interval (<5 minutes)
  - the same OS
  - no overlapping sessions
  - IP activity in 24 hours

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8,476</td>
<td>6,033</td>
<td>10,795</td>
</tr>
<tr>
<td>3</td>
<td>697</td>
<td>523</td>
<td>1,045</td>
</tr>
<tr>
<td>4</td>
<td>108</td>
<td>60</td>
<td>150</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

- RK2015 7 voter group: Colombian IP, ID cards, 20 minutes
- This is a technical upper-bound to group-voting
IP address shared by several verifiers

On average one IP shared by:

- KOV2013: 1.35 verifiers
- EP2014: 1.31 verifiers
- RK2015: 1.4 verifiers

Top IPs shared by:

- KOV2013: 10 verifiers
- EP2014: 13 verifiers
- RK2015: 11 verifiers

Voting and verification IP the same:

- KOV2013: 53.28%
- EP2014: 56.82%
- RK2015: 60.17%
Large percentage of revoters

Voters casting more than one vote:

- KOV2013: 1.93% (2,586 voters)
- EP2014: 1.69% (1,743 voters)
- RK2015: 2.29% (4,034 voters)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>41</td>
<td>60</td>
</tr>
<tr>
<td>27</td>
<td>39</td>
<td>37</td>
</tr>
<tr>
<td>10</td>
<td>36</td>
<td>29</td>
</tr>
<tr>
<td>10</td>
<td>28</td>
<td>19</td>
</tr>
<tr>
<td>9</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>8</td>
<td>17</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Top 10 revoters
Large percentage of revoters

- 30% revote in the first ten minutes
- 40% revote in the first hour
- 20% revote from a different IP
- Voters with parallel voting sessions:
  - KOV2013: 60 voters
  - EP2014: 28 voters
  - RK2015: 99 voters
Large percentage of revoters

KOV2013

EP2014

RK2015
Voting sessions too slow

More than 50% sessions shorter than two minutes
More than 90% sessions shorter than six minutes

The longest voting sessions:
- KOV2013: 4.72 days
- EP2014: 5.6 days
- RK2015: 5.5 days (unsuccessful)
Vote verified from different IP addresses

Votes verified from more than one IP address:

- **KOV2013**: 19
  - 2 IPs (18)
  - 3 IPs (1)
- **EP2014**: 23
  - 2 IPs (23)
- **RK2015**: 49
  - 2 IPs (44)
  - 3 IPs (2)
  - 4 IPs (1)
  - 7 IPs (1)
  - 8 IPs (1)

Verifications over several days from different OSs

⇒ QR codes published somewhere!
Vote verified from different IP addresses – RK2015 4 IPs

https://www.youtube.com/watch?v=yZ4s95lFkk4#t=107
Vote verified from different IP addresses – RK2015 8 IPs

It took less than 1 minute to e-vote @Estonian Parliamentary 2015 election. I'm proud of e-Estonia.

https://twitter.com/LauriBambus/status/568355079318835200/photo/1
First voting session seen as revoting

Security feature. No cases have been registered by the NEC.
Non-i-voter denied paper vote

On election Sunday I-voter will be denied paper vote. Security feature. No cases have been registered by the NEC.
General statistics – voter activity by age

KOV2013

EP2014

RK2015
General statistics – gender distribution of voting

- KOV2013
- EP2014
- RK2015

- % of voters
  - Female
  - Male

KOV2013: 50% Female, 50% Male
EP2014: 50% Female, 50% Male
RK2015: 50% Female, 50% Male
General statistics – voter activity by gender (out of eligible)

In KOV2013 I-voted:
  - M: 12.94%
  - F: 11.78%

In EP2014 I-voted:
  - M: 11.55%
  - F: 9.84%

In RK2015 I-voted:
  - M: 19.54%
  - F: 17.40%
General statistics – age vs voting time

KOV2013

EP2014

RK2015
General statistics – verifier activity by age

KOV2013

EP2014

RK2015
General statistics – gender distribution of verification

- KOV2013
- EP2014
- RK2015

% of verifiers

- Female
- Male

KOV2013: 34% Female, 66% Male
EP2014: 34% Female, 66% Male
RK2015: 34% Female, 66% Male
General statistics – verifier activity by gender

In KOV2013 verified:
- M: 4.87%
- F: 2.04%

In EP2014 verified:
- M: 6.26%
- F: 2.11%

In RK2015 verified:
- M: 6.16%
- F: 2.64%
Verification activity among Mobile-ID users

![Bar chart showing verification activity among Mobile-ID and Non-Mobile-ID users.](chart.png)
General statistics – OS popularity by age

KOV2013

EP2014

RK2015
General statistics – OS popularity by gender

KOV2013

EP2014

RK2015
General statistics – Verification OS popularity (RK2015)

![Graph showing the age distribution and OS popularity across different age groups and genders.]
General statistics – eID tool popularity by age

KOV2013

EP2014

RK2015
General statistics – eID tool popularity by gender

KOV2013

EP2014

RK2015
Conclusions

- Systematic data analysis method has been developed
- Several bugs were found and fixed
- No large-scale attacks were detected against the i-voters
- Observations are similar between the elections
- Interesting phenomena were observed

Limitations

- Some data not available for investigation
- Attack vs legitimate behaviour
- Unexplained voter behaviour