Security Analysis of the Estonian Internet Voting System

Drew Springall, Travis Fkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman
Internet Voting?
Internet Voting in Estonia

Percent of votes cast online

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>2</td>
<td>5</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>National</td>
<td>2</td>
<td>5</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>European</td>
<td>2</td>
<td>5</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>20</td>
<td>30</td>
</tr>
</tbody>
</table>

Election
Estonia gets to vote online. Why can't America?

By Brad Plumer  November 6, 2012

If anecdotal reports are anything to go by, millions of Americans on Tuesday are standing in the cold for hours to vote at their local polling places. But why should they have to? Many Americans can already pay their utilities online and bank online. Why can't we vote over the Internet as well?
◆ Is Estonia’s Internet voting system secure against attackers the country may face?
◆ What is a realistic threat model for a national Internet voting system?
◆ What can other countries considering Internet voting learn from Estonia?
◆ Motivation

◆ How Estonia’s system works
  ◆ Proper Threat Model
  ◆ Analysis
  ◆ Estonian Response
  ◆ Conclusions
Election Servers

Voting Client

Voting Process
Voting Process

Election Servers

Voting Client
Voting Process

Election Servers

Voting Client
**Voting Process**

Inner Envelope:

\[\text{Encrypt}(PK_{\text{elect}}, \text{Pad}_r(\text{Ballot}))\]

Outer Envelope:

\[\text{Sign}(SK_{\text{voter}}, \text{Inner Envelope})\]
Voting Process

Election Servers

Voting Client

Teie tehtud valik läks arvesse.

Soovi korral saate häält muuta uuesti elektrooniliselt hääletades. Arvesse võetakse viimane hääl.

Häält saate muuta ka eelhääletamise ajal valimisjaoks konnas hääletades. Sel juhul võetakse arvesse Teie paberhääl ja elektrooniline hääl tühistatakse. Valimispäeval (26. oktoober) oma häält muuta ei saa!

Häale korrektset kohejoendist on soovi korral võimalik kontrollida Android-tüüpi nutiseadmega. Seleks käivitage nutiseadmes rakendus "Valimised" (saadaval Google Play-s) ja siitgi paremal asuvat QR-koodi. Häält on võimalik kontrollida 30 minuti jooksul kuni kolmel korral.

Palun sulgege rakendus. Turvalisuse huvides eemaldage ID-kaart lugejast!
Verification Process

Election Servers

Voting Client

Verify App
Verification Process

Election Servers

Voting Client

Verify App

Inner Envelope:

\[ \text{Encrypt}(PK_{\text{elect}}, \text{Pad}_r(\text{Ballot})) \]

Outer Envelope:

\[ \text{Sign}(SK_{\text{voter}}, \text{Inner Envelope}) \]
Verification Process

\[ E = \text{Encrypt}(\text{Pk}_{\text{elect}}, \text{Pad}_1(\text{“Paul Politician”})) \]
\[ B = \text{Encrypt}(\text{Pk}_{\text{elect}}, \text{Pad}_1(\text{“Polly Politician”})) \]
\[ B = \text{Encrypt}(\text{Pk}_{\text{elect}}, \text{Pad}_1(\text{“Dictator Drew”})) \]
Verification Process

Election Servers

Voting Client

Verify App

Encrypt(Pk_{\text{elect}}, \text{Pad}_r(\text{“Paul Politician”}))

Encrypt(Pk_{\text{elect}}, \text{Pad}_r(\text{“Dictator Drew”}))

Encrypt(Pk_{\text{elect}}, \text{Pad}_r(\text{“Polly Politician”})))
Verification Process

Election Servers

Voting Client

Verify App

Tuvästatud valik

Rakendus sulgub 23 sekundi pärast!

Kelle valite kohaliku omavalitsuse volikogusse?

Polly Politician

Power to the People Party
Tally Process

Election Servers

Counting Server

Voting Client

Verify App
Tally Process

Election Servers

Counting Server

Voting Client

Verify App
Tally Process
Tally Process
Tally Process

Election Servers

Counting Server

Voting Client

Verify App
Tally Process

- Election Servers
  - Voting Client
  - Verify App
- Counting Server

<table>
<thead>
<tr>
<th>Political party or independent candidate</th>
<th>VOTES</th>
<th>% Of votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonian Reform</td>
<td>79,849</td>
<td>24.3%</td>
</tr>
<tr>
<td>Estonian Centre Party</td>
<td>73,419</td>
<td>22.4%</td>
</tr>
<tr>
<td>Pro Patria and Res Publica Union</td>
<td>45,765</td>
<td>13.9%</td>
</tr>
</tbody>
</table>
Motivation

How Estonia’s system works

Proper Threat Model

Analysis

Estonian Response

Conclusions
◆ Motivation
◆ How Estonia’s system works
◆ Proper Threat Model

◆ Analysis
◆ Estonian Response
◆ Conclusions
Analysis Approaches

The intention behind this repository is to make source code of the server side components of Estonian internet-voting system available for public review.

The repository is not used for active development, but will be kept up to date, so the code that can be found here is the code that is used for election. As the voting system used for legally binding elections must strictly follow the legislation, the actual development of Estonian i-voting system is supervised by National Electoral Committee (NEG) and Internet Voting Committee (www.vvk.ee). The current partner for NEC is Cybernatica AS (www.cyber.ee).

Additional information on the source code can be found on the NEC website: http://www.vvk.ee/valijate-e-haalitamine/

Those, who are not familiar with Estonian language may refer to the following website, which contains subset of the information in English: http://www.vvk.ee/voting-methods-in-estonia/
Observational Approach

- Observed 2013 Local Elections
- Interviewed election officials, developers, and researchers
- Reviewed 20+ hours of official election videos
- Studied written procedures
OPSEC Failures

ID card PINs on camera

Root password on camera
OPSEC Failures

Voting Client built on personal computer

Personal USB stick used for transferring results
Technical Approach

- Reproduced system in lab
- Core of server source code available on GitHub
- Patched voting client
- Built proof-of-concept attacks
Client Infection Method
Client Infection Method

Infect voting client
Client-side Attack

Election Servers

Voting Client

Verify App

- Power to the People Party
  - Polly Politician
- More Power to the People Party
  - Paul Politician
  - All the power to Drew Party
  - Dictator Drew

Kelle valite kohaliku omavalitsuse volikogusse?

Teie valimisringkond:
  - Tallinn

Minu valik on:
  - kandidaat nr 0
  - Polly Politician
  - Power to the People Party

Katkestan
Valin
Client-side Attack

- Election Servers
- Voting Client
- Verify App

Election Servers

Verify App

Voting Client

Client-side attack diagram illustrating the interaction between election servers, verify app, and voting client.
Client-side Attack

Election Servers

Voting Client

Verify App

Tuvastatud valik

Rakendus sulgub 23 sekundi pärast!

Kelle valite kohaliku omavalitsuse volikogusse?

Polly Politician

Power to the People Party
Client-side Attack
Client-side Attack

Election Servers

Voting Client

Verify App
Client-side Attack

Election Servers

Voting Client

Verify App

B

B

B
Client-side Attack

Election Servers

Voting Client

Verify App
Server Infection Method

- Votes stripped and exported to the Counting Server
- HSM decrypts votes and returns to be counted
- OS ISO stored on Dev Server
- Attack Dev Server
  - Inject malware into OS ISO
  - Election officials spread malware during Configuration Ceremony
Server-side Attack

```
try:
    exit_code = subprocess.call([self.decrypt_prog] + args)
except OSError, oserr:
```
◆ Motivation
◆ How Estonia’s system works
◆ Proper Threat Model
◆ Analysis
◆ Estonian Response
◆ Conclusions
Politician Response

Prime Minister Taavi Rõivas

President Toomas Hendrik Ilves

Facebook says they’re agents of the [other] party

Our security is better than Google’s
b) Avaldamata on ainult kliendi lähtekood. Ja seda ei peagi tegema – avatud koodiga verifitseerimisrakendus tuvastab kliendi ebatõepärase käitumise niikuinii

Keylogger pole uus avastus. Aga kui PINi varastada, siis pigem juba rahalise kasu saamiseks (Internetipank, digiallikirjestamine) ja sellised ründed tuleksid välja valimistest sõltumatult. Ravi on pinpadiga lagerid.
Verification app detects all bad behavior.

Keylogger pole uus avastus. Aga kui PINi varastada, siis pigem juba rahalise kasu saamiseks (Internetipank, digiallkirjastamine) ja sellised ründed tuleksid välja valimistest sõltumatult. Ravi on pinpadiga lugerid.
Verification app detects all bad behavior.

Why steal votes when you can steal money?
“nice people who care about computer hygiene have no viruses”

“In practice, computer risks have been eliminated”

“they’re here not because of their technical savvy, but their politically suitable (although technically incompetent) message”
Motivation

How Estonia’s system works

Proper Threat Model

Analysis

Estonian Response

Conclusions
Conclusions

- Threat model should include state-level attackers.
- Attackers could exploit Estonian system to alter results.
  - Major weaknesses are architectural and not easily fixed.
- Lax operational security observed in many areas.
  - Possibly a practical reality of implementation.
- **Recommendation**: Estonia should discontinue Internet voting until there are fundamental technical advances.
Security Analysis of the Estonian Internet Voting System

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman
Backup slides

STOP
Voting Protocol

Voting Client

Election Servers

**TLS Client Auth**

Verify if eligible voter
Find set of candidates $C$

Voter picks candidate $c \in C$
$r \leftarrow \{0, 1\}^{160}$
$b \leftarrow \text{Enc}_{PK_{\text{elect}}}(\text{Pad}_r(c))$
$\sigma \leftarrow \text{Sign}_{SK_{\text{voter}}}(b)$
$v := (b, \sigma)$

Assign $v$ vote ID $x$

Display QR code: $(x, r)$
Verify Protocol

Verification App

Scan QR code \((x, r)\)

Election Servers

Find ballot \(b\) with vote ID \(x\)
Find set of candidates \(C\)

if \(\exists c'\) s.t. \(b = \text{Enc}_{\text{PK}_{\text{elect}}} (\text{Pad}_r(c'))\):
  Display \(c'\)
  Voter checks: \(c' \stackrel{?}{=} c\)
else: Display error
Counting Protocol

**Storage Server**

\[
B \leftarrow \emptyset \\
\text{For each vote } v: \\
(b, \sigma) := v \\
\text{Verify}_{\text{PK}_{\text{voter}}}(b, \sigma) \\
B \leftarrow B \cup \{b\}
\]

**Counting Server**

\[
\text{For each } c \in C: \\
\text{count}_{c}[c] \leftarrow 0 \\
\text{For each } b \in B: \\
c \leftarrow \text{Dec}_{\text{SK}_{\text{elect}}}(b) \\
\text{count}_{c}[c] \leftarrow \text{count}_{c}[c] + 1 \\
\text{Output } \text{count}_{c}
\]