Privacy in Voting

Hugo Jonker

in collaboration with Sjouke Mauw and Jun Pang

hugo.jonker@uni.lu
SaToSS group, University of Luxembourg
overview

- Privacy is tricky (examples)
- Formalise setting
- Understanding privacy
- Define privacy
- Attacking privacy
- What did we miss?
Dutch elections

Dutch ballot:

<table>
<thead>
<tr>
<th></th>
<th>CDA</th>
<th></th>
<th></th>
<th>18. SGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>X</td>
<td></td>
<td></td>
<td>18-1. X'</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-13</td>
<td>Y</td>
<td></td>
<td></td>
<td>18-13. Y'</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-45</td>
<td>Z</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Parties: CDA, VVD, PvdA, SP, Groenlinks, Wilders, LPF, Christenunie, SGP, ...
Privacy is more than “for whom you voted”.
Luxembourgian elections

Luxembourgian ballot:

<table>
<thead>
<tr>
<th></th>
<th>ADR</th>
<th></th>
<th></th>
<th>KPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>J. Henckes</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-21</td>
<td>F. Zeutzius</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-21</td>
</tr>
</tbody>
</table>
 Luxembourgian elections

Luxembourgian ballot:

<table>
<thead>
<tr>
<th>1.</th>
<th>ADR</th>
<th>...</th>
<th>7.</th>
<th>KPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1.</td>
<td>J. Henckes</td>
<td>□ □</td>
<td>...</td>
<td>7-1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-21.</td>
<td>F. Zeutzius</td>
<td>□ □</td>
<td>...</td>
<td>7-21.</td>
</tr>
</tbody>
</table>

- voter marks 21 boxes.
Luxembourgian elections

Luxembourgian ballot:

<table>
<thead>
<tr>
<th></th>
<th>1. ADR</th>
<th>...</th>
<th>7. KPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1.</td>
<td>J. Henckes</td>
<td>■ ■</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>1-21.</td>
<td>F. Zeutzius</td>
<td>□ □</td>
<td>...</td>
</tr>
</tbody>
</table>

- voter marks 21 boxes.
Luxembourgian elections

**Luxembourgian ballot:**

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>ADR</td>
<td>...</td>
<td>7.</td>
<td>KPL</td>
<td></td>
</tr>
<tr>
<td>1-1.</td>
<td>J. Henckes</td>
<td>□</td>
<td>□</td>
<td>...</td>
<td>7-1.</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-21.</td>
<td>F. Zeutzius</td>
<td>□</td>
<td>□</td>
<td>...</td>
<td>7-21.</td>
</tr>
</tbody>
</table>

- voter marks 21 boxes.
- pick 2. That leaves \( \binom{292}{19} = 314,269,098,408,967,151,724,980,483,800 \) ways to fill in ballot.
Privacy is more than “for whom you voted”.

Privacy depends on all knowledge you have.
helpful voters
Privacy is more than “for whom you voted”.

Privacy depends on all knowledge you have.

Subjects may seek to reduce/renounce privacy.
- Quantify privacy.
- Taking conspiring voters into account.
- Based on the intruder’s knowledge.
**quantifying privacy**

choice group $cg_v$: contains all candidates, that a voter $v$ might have chosen.
quantifying privacy

choice group $cg_v$:
contains all candidates, that a voter $v$ might have chosen.

Example:
$C = \{ Vike - Freiberga, Balkenende, Juncker \}$.

- results: Balkenende 0 votes
  $\implies \forall v \in V: cg_v(\forall S) = \{ Juncker, Vike - Freiberga \}$.

- $v$ voted for a man
  $\implies cg_v(\forall S) = \{ Balkenende, Juncker \}$.
conspiring voters

- Extra info: what the intruder doesn’t know.
- The intruder sees communications.
- So: initial/final knowledge, untappable channels.
Indistinguishability:
a series of events \( t \) is indistinguishable from a series \( t' \) if
“the intruder cannot distinguish them”.
Indistinguishability:
a series of events $t$ is indistinguishable from a series $t'$ if
“the intruder cannot distinguish them”.

Example:

- Encryption: $\{c\}_k \sim \{c'\}_k$, if the intruder does not know $k$.
- Nonces: $\{n\}_k \sim \{n'\}_k$, always.
Terms:

\[ \varphi ::= \text{var} \in \text{Vars} \mid c \in \mathcal{C} \mid n \in \text{Nonces} \mid k \mid (\varphi_1, \varphi_2) \mid \{\varphi\}^k. \]

- voters \( v \in \mathcal{V} \)
- choice function \( \gamma: \mathcal{V} \rightarrow \mathcal{C} \)
- \( vc \in \text{Vars} \): voter’s choice
knowledge

\[ K \cup \{ \varphi \} \vdash \varphi \]
\[ K \vdash \varphi_1, K \vdash \varphi_2 \quad \implies \quad K \vdash (\varphi_1, \varphi_2) \]
\[ K \vdash (\varphi_1, \varphi_2) \quad \implies \quad K \vdash \varphi_1, K \vdash \varphi_2 \]
\[ K \vdash \varphi_1, K \vdash k \quad \implies \quad K \vdash \{ \varphi_1 \}_k \]
\[ K \vdash \{ \varphi_1 \}_k, K \vdash k^{-1} \quad \implies \quad K \vdash \varphi_1 \]

closure: \[ \overline{K} = \{ \varphi \mid K \vdash \varphi \} \]
Events:

\[ E_v = \{ \begin{align*} s(a, a', \varphi), & \quad r(a, a', \varphi), \\ as(a, a', \varphi), & \quad ar(a', \varphi), \\ us(a, a', \varphi), & \quad ur(a, a', \varphi), \\ ph(i) & \end{align*} \} \]

\[ | a, a' \in\text{Agents}, \varphi \in\text{Terms}, i \in \mathbb{N} \].
communication

Events:

\[ Ev = \{ s(a, a', \varphi), r(a, a', \varphi), as(a, a', \varphi), ar(a', a, \varphi), us(a, a', \varphi), ur(a', a, \varphi), \phi(i) \mid a, a' \in \text{Agents}, \varphi \in \text{Terms}, i \in \mathbb{N} \}. \]

Event order:

\[ P ::= \delta \mid ev.P \mid P_1 + P_2 \mid P_1 < \varphi_1 = \varphi_2 > P_2 \mid ev.X(\varphi_1, \ldots, \varphi_n) \]
**voting system**

**Definition 1 (voting system)** A *voting system* \( \mathcal{V} \in \text{VotSys} \) specifies the state of each agent:

\[
\text{VotSys} = \text{Agents} \rightarrow (\mathcal{P} (\text{Terms}) \times \text{Processes}).
\]

Specifying choice:

\[
\mathcal{V}^\gamma(a) = \begin{cases} 
\mathcal{V}(a) & \text{if } a \notin \mathcal{V} \\
(\pi_1(\mathcal{V}(a)), \sigma_a(\pi_2(\mathcal{V}(a)))) & \text{if } a \in \mathcal{V}
\end{cases}
\]

where \( \sigma_a = \text{vc} \mapsto \gamma(a) \).
modelling privacy

When can the intruder distinguish $Tr(\mathcal{VS}^{\gamma_1})$ from $Tr(\mathcal{VS}^{\gamma_2})$?

When he can **reinterpret** $t$ as $t'$.
**reinterpretation**

**Definition 2 (reinterpretation (GHPR05))** Let \( \rho \) be a permutation on the set of terms \( Terms \) and let \( K_I \) be a knowledge set. The map \( \rho \) is a **semi-reinterpretation under** \( K_I \) if it satisfies the following.

\[
\begin{align*}
\rho(p) &= p, \text{ for } p \in C \cup Keys \\
\rho((\varphi_1, \varphi_2)) &= (\rho(\varphi_1), \rho(\varphi_2)) \\
\rho(\{\varphi\}_k) &= \{\rho(\varphi)\}_k, \text{ if } K_I \vdash \varphi, k \lor K_I \vdash \{\varphi\}_k, k^{-1}
\end{align*}
\]

Map \( \rho \) is a **reinterpretation under** \( K_I \) iff it is a semi-reinterpretation and its inverse \( \rho^{-1} \) is a semi-reinterpretation under \( \rho(K_I) \).
Traces $t, t'$ are indistinguishable for the intruder, notation $t \sim t'$ iff there exists a reinterpretation $\rho$ such that

$$obstr(t') = \rho(obstr(t)) \land \overline{K_I^t} = \rho(\overline{K_I^{t'}}).$$
Given voting system $\mathcal{VS}$, choice functions $\gamma_1, \gamma_2$ are indistinguishable to the intruder, notation $\gamma_1 \simeq_{\mathcal{VS}} \gamma_2$ iff

\begin{align*}
\forall t \in Tr(\mathcal{VS}^{\gamma_1}) : \exists t' \in Tr(\mathcal{VS}^{\gamma_2}) : t \sim t' \quad \land \\
\forall t \in Tr(\mathcal{VS}^{\gamma_2}) : \exists t' \in Tr(\mathcal{VS}^{\gamma_1}) : t \sim t'
\end{align*}
The choice group for a voting system $\mathcal{V}$ and a choice function $\gamma$ is given by

$$cg(\mathcal{V}, \gamma) = \{ \gamma' \mid \gamma \simeq_{\mathcal{V}} \gamma' \}.$$ 

The choice group for a particular voter $v$, i.e. the set of candidates indistinguishable from $v$’s chosen candidate, is given by

$$cg_v(\mathcal{V}, \gamma) = \{ \gamma'(v) \mid \gamma' \in cg(\mathcal{V}, \gamma) \}.$$
Introduction

Privacy = tricky

Understanding privacy

Formalizing

Defining privacy

Attacking privacy

- conspiracy
- event transformation
- process transformation
- conspiracy-resistance

Wrapping up

---

**conspiracy**

Diagram:

1. classic-rf
   \[\text{vote-priv}\]

2. start-rf

a. rf-share
b. rf-witness

(i)

(c. rf-relay

(ii)
transform processes using $\Theta_i$, where $i \in \{1, 2, a, b, c\}$.

transform events using $\theta_i$

coercion-resistance $i$:
\[
\forall v, \gamma : cg^i_v(\mathcal{VS}, \gamma) = cg_v(\Theta_i(v, \mathcal{VS}), \gamma)
\]
event transformation

\[ \theta_a(v, ev) = \begin{cases} 
ur(a_g, v, \varphi) \cdot is(v, \varphi) & \text{if } ev = ur(a_g, v, \varphi) \\
 ev & \text{otherwise}
\end{cases} \]

\[ \theta_c(v, ev) = \theta_b(v, \theta_a(v, ev)) \]
θ_2(v, P) = is(knω_v).P

θ_i(v, P) = θ_i(v, P_1) ◁ ϕ_1 = ϕ_2 ▷ θ_i(v, P_2)

if \[ P = P_1 ◁ ϕ_1 = ϕ_2 ▷ P_2, \]

for \[ ϕ_1, ϕ_2 ∈ Terms \]
### conspiracy-resistance

#### classical notion:

\[
\forall v, \gamma : |cg_v^1(\mathcal{VS}, \gamma)| > 1.
\]

#### New: conspiracy-dependent notion:

\(\forall \mathcal{S}\) is **conspiracy-resistant** for conspiring behaviour \(i \in \{1, 2, a, b, c\}\) iff

\[
\forall v \in \mathcal{V}, \gamma \in \mathcal{V} \rightarrow \mathcal{C} : cg_v^i(\mathcal{VS}, \gamma) = cg_v(\mathcal{VS}, \gamma).
\]
concluding

- we can quantify privacy in voting
- possibility to detect new attacks
- choice group aids reasoning about privacy
concluding

- we can quantify privacy in voting
- possibility to detect new attacks
- choice group aids reasoning about privacy

Future work:

- conspiring authorities
- defense strategies
- automated verification
- extend with probabilism (election result)
Thank you for your attention.

Questions?