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:

1. CDA	· · ·	18. SGP
1-1. X ☐	· · ·	18-1. X' ☐
⋮	⋮	⋮
1-13. Y ☐		18-13. Y' ☐
⋮	⋮	
1-45. Z ☐	· · ·	

Parties: CDA, VVD, PvdA, SP, Groenlinks, Wilders, LPF, Christenunie, SGP, . . .

- Privacy is more than “for whom you voted”.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	···	7. KPL
1-1. J. Henckes ☐ ☐	···	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	···	7-21. M. Tani ☐ ☐

Luxembourgian elections

Luxembourgian ballot:

1.	ADR			···	7.	KPL		
1-1.	J. Henckes	□	□	···	7-1.	P. Back	□	□
⋮				⋮	⋮			
1-21.	F. Zeutzius	□	□	···	7-21.	M. Tani	□	□

- voter marks 21 boxes.

Luxembourgian elections

Luxembourgian ballot:

1.	ADR				· · ·	7.	KPL						
1-1.	J. Henckes	■	■		· · ·	7-1.	P. Back	□	□				
	⋮				⋮		⋮						
1-21.	F. Zeutzius	□	□		· · ·	7-21.	M. Tani	□	□				

- voter marks 21 boxes.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	$\cdots$	7. KPL
1-1. J. Henckes ■ ■	$\cdots$	7-1. P. Back □ □
$\vdots$	$\vdots$	$\vdots$
1-21. F. Zeutzius □ □	$\cdots$	7-21. M. Tani □ □

- 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.

lesson

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

helpful voters

lesson

- Privacy is more than “for whom you voted”.
- Privacy depends on all knowledge you have.
- Subjects may seek to reduce/renounce privacy.

approach

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

- results: Balkenende 0 votes
  $\implies \forall v \in \mathcal{V}\colon\ cg_v(\mathcal{VS}) = \{Juncker, Vike-Freiberga\}$.
- v voted for a man
  $\implies cg_v(\mathcal{VS}) = \{Balkenende, Juncker\}$.

conspiring voters

- Extra info: what the intruder doesn't know.
- The intruder sees communications.
- So: initial/final knowledge, untappable channels.

private from intruder

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.

syntax

Terms:

$$\varphi ::= \mathsf{var} \in \mathsf{Vars} \mid c \in \mathcal{C} \mid n \in Nonces \mid k \mid (\varphi_1, \varphi_2) \mid \{\varphi\}_k.$$

- voters $v \in \mathcal{V}$
- choice function $\gamma \colon \mathcal{V} \to \mathcal{C}$
- vc $\in$ Vars: voter's choice

knowledge

$$K \cup \{\varphi\} \vdash \varphi$$

$$K \vdash \varphi_1,\ K \vdash \varphi_2 \implies K \vdash (\varphi_1, \varphi_2)$$

$$K \vdash (\varphi_1, \varphi_2) \implies K \vdash \varphi_1,\ K \vdash \varphi_2$$

$$K \vdash \varphi_1,\ K \vdash k \implies K \vdash \{\varphi_1\}_k$$

$$K \vdash \{\varphi_1\}_k,\ K \vdash k^{-1} \implies K \vdash \varphi_1$$

closure: $\overline{K} = \{\varphi \mid K \vdash \varphi\}$

Events:

$$
\begin{aligned}
Ev = \{ \quad & s(a, a', \varphi), \quad r(a, a', \varphi), \\
& as(a, a', \varphi), \quad ar(a', \varphi), \\
& us(a, a', \varphi), \quad ur(a, a', \varphi), \\
& ph(i) \\
& \mid a, a' \in Agents, \varphi \in Terms, i \in \mathbb{N}\}.
\end{aligned}
$$

communication

Events:

$$
\begin{aligned}
Ev = \{ \quad & s(a, a', \varphi), \quad r(a, a', \varphi), \\
& as(a, a', \varphi), \quad ar(a', \varphi), \\
& us(a, a', \varphi), \quad ur(a, a', \varphi), \\
& ph(i) \\
& \mid a, a' \in Agents, \varphi \in Terms, i \in \mathbb{N}\}.
\end{aligned}
$$

Event order:

$$
P \quad ::= \quad \delta \mid ev.P \mid P_1 + P_2 \mid P_1 \lhd \varphi_1 = \varphi_2 \rhd P_2 \mid ev.X(\varphi_1, \ldots, \varphi
$$

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

$$VotSys = Agents \rightarrow (\mathcal{P}(Terms) \times Processes).$$

Specifying choice:

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

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

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 ρ be a permutation on the set of terms $\mathcal{Terms}$ and let K_I be a knowledge set. The map ρ is a* <u>*semi-reinterpretation under K_I*</u> *if it satisfies the following.*

$$\begin{array}{rcl} \rho(p) & = & p, \text{ for } p \in \mathcal{C} \cup Keys \\ \rho((\varphi_1, \varphi_2)) & = & (\rho(\varphi_1), \rho(\varphi_2)) \\ \rho(\{\varphi\}_k) & = & \{\rho(\varphi)\}_k, \text{ if } K_I \vdash \varphi, k \vee K_I \vdash \{\varphi\}_k, k^{-1} \end{array}$$

Map ρ is a <u>*reinterpretation under K_I*</u> *iff it is a semi-reinterpretation and its inverse ρ^{-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 ρ such that

$$obstr(t') = \rho(obstr(t)) \ \wedge \ \overline{K_I^t} = \rho(\overline{K_I^{t'}}).$$

choice privacy

Given voting system $\mathcal{VS}$, choice functions γ_1, γ_2 are indistinguishable to the intruder, notation $\gamma_1 \simeq_{\mathcal{VS}} \gamma_2$ iff

$$\forall t \in Tr(\mathcal{VS}^{\gamma_1}) : \exists t' \in Tr(\mathcal{VS}^{\gamma_2}) : t \sim t' \quad \wedge$$
$$\forall t \in Tr(\mathcal{VS}^{\gamma_2}) : \exists t' \in Tr(\mathcal{VS}^{\gamma_1}) : t \sim t'$$

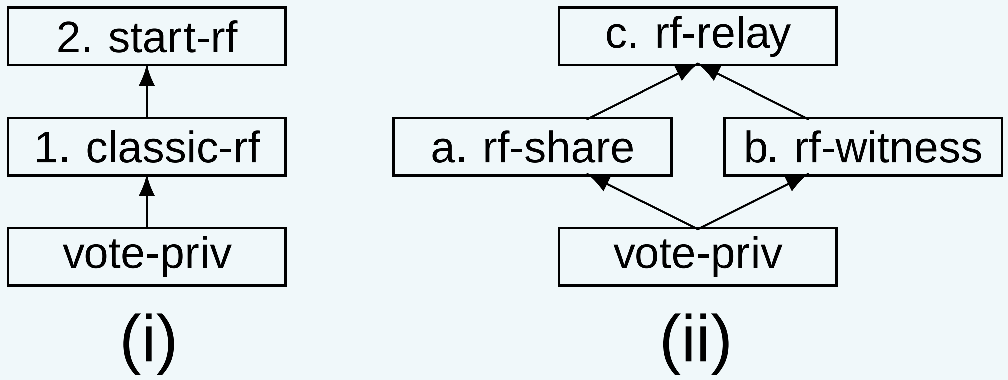
The choice group for a voting system $\mathcal{VS}$ and a choice function γ is given by

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

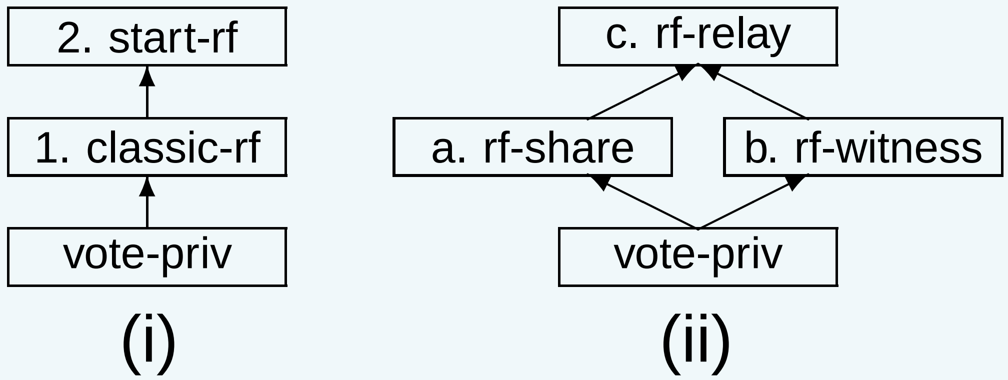
The choice group for a particular voter v, i.e. the set of candidates indistinguishable from v's chosen candidate, is given by

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

conspiracy


2. start-rf
1. classic-rf
vote-priv
(i)
c. rf-relay
a. rf-share
b. rf-witness
vote-priv
(ii)

conspiracy



- transform processes using Θ_i, where $i \in \{1, 2, a, b, c\}$.
- transform events using θ_i
- coercion-resistance i:
  $\forall v, \gamma \colon \; cg_v^i(\mathcal{VS}, \gamma) = cg_v(\Theta_i(v, \mathcal{VS}), \gamma)$

event transformation

$$\theta_a(v, ev) = \begin{cases} ur(ag, v, \varphi) \;.\; is(v, \varphi) & \text{if } ev = ur(ag, v, \varphi) \\ ev & \text{otherwise} \end{cases}$$

$$\theta_c(v, ev) = \theta_b(v, \theta_a(v, ev))$$

process transformation

$$\Theta_2(v, P) = is(knw_v).P$$

$$\Theta_i(v, P) = \Theta_i(v, P_1) \lhd \varphi_1 = \varphi_2 \rhd \Theta_i(v, P_2)$$

if $P = P_1 \lhd \varphi_1 = \varphi_2 \rhd P_2,$

for $\varphi_1, \varphi_2 \in Terms$

conspiracy-resistance

classical notion:

$$\forall v, \gamma \colon \left| cg_v^1(\mathcal{VS}, \gamma) \right| > 1.$$

New: conspiracy-dependent notion:

$\mathcal{VS}$ is conspiracy-resistant for conspiring behaviour $i \in \{1, 2, a, b, c\}$ iff

$$\forall v \in \mathcal{V}, \gamma \in \mathcal{V} \to \mathcal{C} \colon \; cg_v^i(\mathcal{VS}, \gamma) = cg_v(\mathcal{VS}, \gamma).$$

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)

final slide

Thank you for your attention.

Questions?