Measuring Voter-controlled Privacy

Hugo Jonker

in collaboration with Sjouke Mauw and Jun Pang

hugo.jonker@uni.lu

SaToSS group, University of Luxembourg

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 □ □

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	□	□

Ways to complete this ballot:

$\binom{292}{19}$ = 314,269,098,408,967,151,724,980,483,800

lesson

Introduction

Privacy = tricky
-Lux elections
-helpful voters

Understanding privacy

Formalizing

Measuring privacy

Wrapping up

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

helpful voters

lesson

Introduction
Privacy = tricky
-Lux elections
-helpful voters
Understanding privacy
Formalizing
Measuring privacy
Wrapping up

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

approach

Introduction
Privacy = tricky
Understanding privacy
-approach
-quantifying privacy
-conspiring voters
-private from intruder
Formalizing
Measuring privacy
Wrapping up

- Quantify privacy.
- Taking conspiring voters into account.
- Based on the intruder’s knowledge.

Introduction
Privacy = tricky
Understanding privacy
-approach
-quantifying privacy
-conspiring voters
-private from intruder
Formalizing
Measuring privacy
Wrapping up

choice group cg_v:

contains all candidates, that a voter v might have chosen.

quantifying privacy

Introduction
Privacy = tricky
Understanding privacy
-approach
-quantifying privacy
-conspiring voters
-private from intruder
Formalizing
Measuring privacy
Wrapping up

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
  $\implies \forall v \in \mathcal{V}\colon Balkenende \notin cg_v(\mathcal{VS})$.
- v voted for a man
  $\implies cg_v(\mathcal{VS}) \subseteq \{Balkenende, Juncker\}$.

conspiring voters

Introduction

Privacy = tricky

Understanding privacy
-approach
-quantifying privacy
-conspiring voters
-private from intruder

Formalizing

Measuring privacy

Wrapping up

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

private from intruder

Introduction
Privacy = tricky
Understanding privacy
-approach
-quantifying privacy
-conspiring voters
-private from intruder
Formalizing
Measuring privacy
Wrapping up

Indistinguishability:

a list of events t is indistinguishable from a list t' if “the intruder cannot distinguish them”.

in a nutshell

Introduction

Privacy = tricky

Understanding privacy

Formalizing

-in a nutshell

-syntax

-modelling privacy

-reinterpretation

-events privacy

-choice privacy

Measuring privacy

Wrapping up

- voters, authorities $\Longrightarrow$ communicating processes
- processes communicate <u>terms</u>
- communication <u>events</u> $\Longrightarrow$ trace
- trace $\xrightarrow{intruder}$ privacy

syntax

Introduction
Privacy = tricky
Understanding privacy
Formalizing
-in a nutshell
-syntax
-modelling privacy
-reinterpretation
-events privacy
-choice privacy
Measuring privacy
Wrapping up

- voters $\mathcal{V}$, candidates $\mathcal{C}$
- choice function $\gamma\colon \mathcal{V} \to \mathcal{C}$

Terms:

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

Introduction
Privacy = tricky
Understanding privacy
Formalizing
-in a nutshell
-syntax
-modelling privacy
-reinterpretation
-events privacy
-choice privacy
Measuring privacy
Wrapping up

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

When he can<u>not</u> **reinterpret** t as t'.

Introduction
Privacy = tricky
Understanding privacy
Formalizing
-in a nutshell
-syntax
-modelling privacy
-reinterpretation
-events privacy
-choice privacy
Measuring privacy
Wrapping up

Definition 1 (reinterpretation (adapted from GHPR05))

Let ρ be a permutation on the set of terms $Terms$ and let K_I be a knowledge set. The map ρ is a semi-reinterpretation under K_I if it satisfies the following.

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

Map ρ is a reinterpretation under K_I iff it is a semi-reinterpretation and its inverse ρ^{-1} is a semi-reinterpretation under $\rho(K_I)$.

events privacy

Introduction
Privacy = tricky
Understanding privacy
Formalizing
-in a nutshell
-syntax
-modelling privacy
-reinterpretation
-events privacy
-choice privacy
Measuring privacy
Wrapping up

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

Introduction

Privacy = tricky

Understanding privacy

Formalizing
-in a nutshell
-syntax
-modelling privacy
-reinterpretation
-events privacy
-choice privacy

Measuring privacy

Wrapping up

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

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

choice group

Introduction
Privacy = tricky
Understanding privacy
Formalizing
Measuring privacy
-choice group
-goals
-conspiracy-resistance
Wrapping up

Possible choices for $\mathcal{VS}, \gamma$:

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

Possible choices for v then:

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

goals

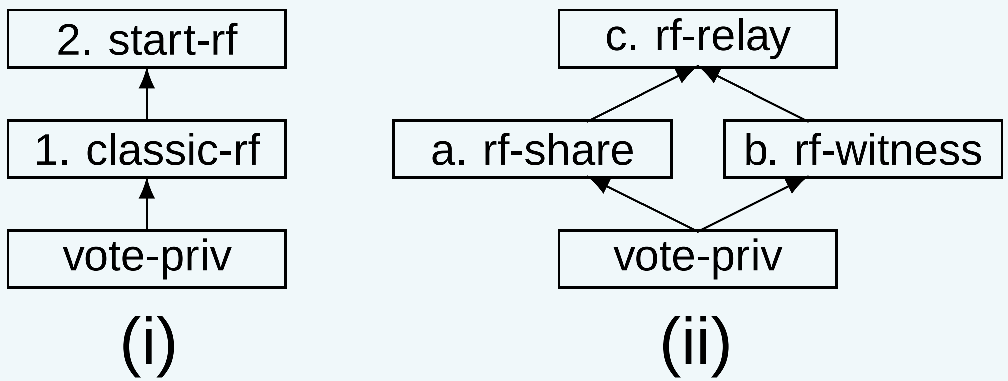
Introduction
Privacy = tricky
Understanding privacy
Formalizing
Measuring privacy
-choice group
-goals
-conspiracy-resistance
Wrapping up

- √ privacy $>$ “for whom you voted”
- √ depends on knowledge
- ? conspiring voter

goals

Introduction
Privacy = tricky
Understanding privacy
Formalizing
Measuring privacy
-choice group
-goals
-conspiracy-resistance
Wrapping up

- √ privacy > "for whom you voted"
- √ depends on knowledge
- ? conspiring voter



conspiracy-resistance

Introduction
Privacy = tricky
Understanding privacy
Formalizing
Measuring privacy
-choice group
-goals
-conspiracy-resistance
Wrapping up

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

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

Introduction
Privacy = tricky
Understanding privacy
Formalizing
Measuring privacy
Wrapping up
-concluding

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)

Introduction
Privacy = tricky
Understanding privacy
Formalizing
Measuring privacy
Wrapping up
-concluding

Thank you for your attention.

Questions?