Privacy in eVoting protocols

(collaborations: dr. E.P. de Vink, prof. dr. S. Mauw, ir. drs. W. Pieters)

Hugo Jonker

hugo.jonker@uni.lu

eVoting

Involved parties:

- voters
- candidates
- voting officials (administrators):
  - counter(s)
  - registrar(s)
  - anonymous channel(s)
  - ...

protocols

Intuitively:

> A prescribed way to exchange messages between parties, in order to achieve a stated goal, satisfying stated requirements.

Note: distinction between roles and parties. From now on: roles.

eVoting protocols

- goal: establish consensus in a group
- requirements:
  - democracy
  - eligibility
  - accuracy
  - verifiability
  - ...
  - privacy

privacy

Two sides to privacy:

- uncertainty
- indistinguishability
  - k-anonymity...
  - ...anonymity groups!!

What is privacy?

what is to be kept private?

- voter?
- link voter-ballot?
- link voter-candidate?
- link ballot-candidate?

existing notions

Existing notions of privacy in eVoting:

- Anonymity
  link voter-ballot cannot be determined by observation
- receipt-freeness
  no proof
- strong receipt-freeness
  no elimination of possibilities
- coercion-resistance
  - no randomisation
  - no abstention
  - no simulation

intuition

A receipt proves how a voter voted.

intuition

A receipt proves how a voter voted.

Examples:

- Everyone signs their vote.

intuition

A receipt proves how a voter voted.

Examples:

- Everyone signs their vote.

- In Italy, simultaneous elections were held for various posts, using one ballot. The order of posts listed is up to the voter, and is preserved. An attacker (El Mafiosi) can assign each voter a specific order of posts.
  Benaloh & Tuinstra

requirements

More precisely: a receipt r proves that a voter v *cast* a vote for candidate c.

requirements

More precisely: a receipt r proves that a voter v *cast* a vote for candidate c.

- R1: r authenticates v

requirements

More precisely: a receipt r proves that a voter v *cast* a vote for candidate c.

- R1: r authenticates v
- R2: r proves that v chose candidate c

requirements

More precisely: a receipt r proves that a voter v *cast* a vote for candidate c.

- R1: r authenticates v
- R2: r proves that v chose candidate c
- R3: r proves that v cast her vote

requirements

More precisely: a receipt r proves that a voter v *cast* a vote for candidate c.

- R1: r authenticates v
- R2: r proves that v chose candidate c
- R3: r proves that v cast her vote

Note:
- for specific types of elections
- quite strict

decomposing receipts

The following functions are used to decompose receipts:

- $\alpha : \mathcal{R} \rightarrow \mathcal{AT}$, extract authentication term from receipt
- $\beta : \mathcal{R} \rightarrow \mathcal{RB}$, extract ballot from receipt
- $\gamma : \mathcal{R} \rightarrow \mathcal{C}$, extract candidate from receipt

Formalisation of the requirements:

decomposing receipts

The following functions are used to decompose receipts:

- $\alpha : \mathcal{R} \rightarrow \mathcal{AT}$, extract authentication term from receipt
- $\beta : \mathcal{R} \rightarrow \mathcal{RB}$, extract ballot from receipt
- $\gamma : \mathcal{R} \rightarrow \mathcal{C}$, extract candidate from receipt

Formalisation of the requirements:

- R1: $\alpha(r) \in \mathcal{AT}(v)$
- R2: $\gamma(r) = \Gamma(v)$
- R3: $\beta(r) \in \mathcal{RB}$

decomposing receipts

The following functions are used to decompose receipts:

- $\alpha : \mathcal{R} \rightarrow \mathcal{AT}$, extract authentication term from receipt
- $\beta : \mathcal{R} \rightarrow \mathcal{RB}$, extract ballot from receipt
- $\gamma : \mathcal{R} \rightarrow \mathcal{C}$, extract candidate from receipt

Formalisation of the requirements:

- R1: $\alpha(r) \in \mathcal{AT}(v)$
- R2: $\gamma(r) = \Gamma(v)$
- R3: $\beta(r) \in \mathcal{RB}$

So, for valid receipts: $auth(\alpha(r)) = v \implies \gamma(r) = \Gamma(v)$, which is satisfied by $\gamma = \Gamma \circ auth \circ \alpha$.

RF ≈ anonymity

Anonymity, 3 flavours:

- sender/voter anonymity?
  no, voter tries to prove vote

RF ≈ anonymity

Anonymity, 3 flavours:

- sender/voter anonymity?
  no, voter tries to prove vote
- plausible deniability?
  no, sender knows how she voted

RF ≈ anonymity

Anonymity, 3 flavours:

- sender/voter anonymity?
  no, voter tries to prove vote
- plausible deniability?
  no, sender knows how she voted
- unlinkability?
  “no link between vote and voter”...

unlinkability

Unlinkability of message m to sender v:

- intruder does not know that v sent m
- intruder cannot rule out that v sent any message m', where $m' \in AS$, the Anonymity Set

unlinkability

Unlinkability of message m to sender v:

- intruder does not know that v sent m
- intruder cannot rule out that v sent any message m', where $m' \in AS$, the Anonymity Set

Strong receipt-freeness
the intruder cannot rule out *any* vote from the anonymity set.

$$t.(v \to \mathsf{spy}\colon r) \quad \models \quad (\neg \Box_{\mathsf{spy}}(v \text{ sends } m)) \quad \wedge \quad \bigwedge_{m' \in AMS} \Diamond_{\mathsf{spy}}(v \text{ sends } m')$$

currently: two approaches

Current situation:

- Delaune, Kremer and Ryan proposed an approach based on bisimilarity
  – ignoring the notion of receipts
- Jonker and De Vink proposed an approach based on the characteristics of a receipt
  – founded on the notion of receipts

future: unifying approach

- branching bisimilarity as an equivalence seems to strong
  e.g. order in which voters vote does not affect rf
- checking terms J&DV-style seems imprecise
  not a precise notion of receipts
- so unite the two!
  construct an appropriate equivalence notion for voting processes based on identifying receipts

future: unifying approach

- branching bisimilarity as an equivalence seems to strong
  e.g. order in which voters vote does not affect rf
- checking terms J&DV-style seems imprecise
  not a precise notion of receipts
- so unite the two!
  construct an appropriate equivalence notion for voting processes based on identifying receipts

Thanks for your attention!