Receipt-Freeness as a Special Case of Anonymity

(joint work with Wolter Pieters)

Hugo Jonker

h.l.jonker@tue.nl

Anonymity in networks

- Defined using an Anonymity Set
- Various definitions, e.g.

Anonymity in networks

- Defined using an Anonymity Set
- Various definitions, e.g.
  - Sender anonymity of sender A w.r.t. message m
    Everyone in the anonymity set could have sent m

Anonymity in networks

- Defined using an Anonymity Set
- Various definitions, e.g.
  - Sender anonymity of sender A w.r.t. message m
    Everyone in the anonymity set could have sent m
  - Unlinkability of sender A and receiver B
    - The adversary (spy) is not sure that A sent any message to B
    - The spy cannot rule out anyone from the anonymity set

Anonymity in networks

- Defined using an Anonymity Set
- Various definitions, e.g.
  - Sender anonymity of sender A w.r.t. message m
    Everyone in the anonymity set could have sent m
  - Unlinkability of sender A and receiver B
    - The adversary (spy) is not sure that A sent any message to B
    - The spy cannot rule out anyone from the anonymity set
  - Plausible deniability of agent A w.r.t. message m
    The spy knows that A does not know that she posesses m

Anonymity in voting

Two related properties:

- Privacy (allows anonymity)
- Receipt-freeness (requires anonymity)

Delaune et al. characterise receipt-freeness as:

> A voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way.

Epistemic logic

Core concepts of receipt-freeness:

- possessing information
- proving another party

Epistemic logic allows to reason about this naturally.

Epistemic logic

Core concepts of receipt-freeness:

- possessing information
- proving another party

Epistemic logic allows to reason about this naturally.

Most epistemic definitions skipped in this talk – see the paper for more details

Similarities

- Anonymity is similar to receipt-freeness
- So, can concepts from anonymity be lifted to receipt-freeness?
  e.g. anonymity sets

Which anonymity?

- Sender anonymity?
- Unlinkability?
- Plausible deniability?

Which anonymity?

- Sender anonymity?
  - No, sender tries to prove something
- Unlinkability?
- Plausible deniability?

Which anonymity?

- Sender anonymity?
  - No, sender tries to prove something
- Unlinkability?

- Plausible deniability?
  - No, sender knows that she possesses m

Which anonymity?

- Sender anonymity?
  - No, sender tries to prove something
- Unlinkability?
  - “no link (receipt) between voter and vote”: OK!
- Plausible deniability?
  - No, sender knows that she possesses m

Unlinkability revisited

Formally, in epistemic logic (framework Garcia et. al.):

Definition 1 *(Unlinkability) A run r provides* unlinkability *for users A and B with anonymity set AS iff*

$$r \models \left(\neg \Box_{\mathsf{spy}} \varphi(A,B)\right) \wedge \bigwedge_{X \in AS} \Diamond_{\mathsf{spy}} \varphi(X,B) \ ,$$

where $\varphi(X,Y) = \exists n.\ \big(X \text{ Sends } n \wedge Y \text{ Possesses } n\big)$.

Weak receipt-freeness

Intuitively: weakly receipt-free means that the voter possesses no message that convinces the spy of how she voted.

Weak receipt-freeness

Intuitively: weakly receipt-free means that the voter possesses no message that convinces the spy of how she voted.

Definition 3 *(Weak receipt-freeness) A run of a protocol is* weakly receipt-free *for agent A with respect to message m iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,*

$$r.(A \rightarrow \mathsf{spy} : m') \models \neg \Box_{\mathsf{spy}}(A \text{ sends } m)$$

Weak receipt-freeness

Intuitively: weakly receipt-free means that the voter possesses no message that convinces the spy of how she voted.

Definition 4 *(Weak receipt-freeness) A run of a protocol is* weakly receipt-free *for agent A with respect to message m iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,*

$$r.(A \rightarrow \mathsf{spy} : m') \models \neg \Box_{\mathsf{spy}}(A \text{ sends } m)$$

Problem: what if the spy knows the voter did *not* vote for the spy's preferred candidate?

Strong receipt-freeness

Intuitively: No matter what information the voter supplies, *any* message (vote) from the anonymity set may have been sent by the voter.

Strong receipt-freeness

Intuitively: No matter what information the voter supplies, *any* message (vote) from the anonymity set may have been sent by the voter.

Definition 6 *(Strong receipt-freeness) A run r of a protocol is* strongly receipt-free *for agent A with respect to a message m in anonymity set AMS iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,*

$$r.(A \to \mathsf{spy} : m') \models (\neg \Box_{\mathsf{spy}}(A \,\mathsf{sends}\, m)) \quad \wedge \bigwedge_{m'' \in AMS} \Diamond_{\mathsf{spy}}(A \,\mathsf{sends}\, m'')$$

Conclusions

- A definition of receipt-freeness based on the intuitive concept
- A stronger definition
- Reasoning about knowledge facilitated by epistemic logic
- Lifting of the concept of anonymity set to receipt-freeness
- More on anonymity and epistemic logic in the paper

Future work

- Validate definitions against known receipt-free protocols
- Alternate definitions based on knowledge of the spy, not extension of a run
- Test untried protocols for receipt-freeness
- Expressing verifiability in epistemic logic

And, since talking to Josh:

- Investigate probabilistic definitions of receiptfreeness
- Investigate probabilistic definitions of anonymity

Future work

- Validate definitions against known receipt-free protocols
- Alternate definitions based on knowledge of the spy, not extension of a run
- Test untried protocols for receipt-freeness
- Expressing verifiability in epistemic logic

And, since talking to Josh:

- Investigate probabilistic definitions of receiptfreeness
- Investigate probabilistic definitions of anonymity

Questions?