Expressing and verifying privacy properties with epistemic logic

Fortunat Rajaona and Ioana Boureanu

Surrey Centre for Cyber Security, University of Surrey, United Kingdom

Recognised Value in Epistemic Expressions of Privacy ...

the main advantage of modal logics of knowledge is that even fairly complex information hiding properties can be stated directly as formulas in the logic

(Hughes and Shmatikov 2004)

epistemic logics are often better suited for expressing certain security properties such as secrecy and anonymity

(Delaune *et al.* 2009)

Epistemic Logic: A Reminder

Syntax

$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_i\varphi$

Kripke Model

$\mathcal{M} = (W, \sim_i, Val)$

W	set of possible worlds
$\sim_i \subseteq W \times W$	indistinguishability relations
$Val : W \to \mathcal{P}(P)$	valuation function

Semantics

$(\mathcal{M}, w) \models K_i\varphi$ iff $w \sim_i w'$ implies $(\mathcal{M}, w') \models \varphi$

Epistemic Logic: A Reminder

Syntax

$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_i\varphi$

Kripke Model

$\mathcal{M} = (W, \sim_i, Val)$

W	set of possible worlds
$\sim_i \subseteq W \times W$	indistinguishability relations
$Val : W \to \mathcal{P}(P)$	valuation function

Semantics

$(\mathcal{M}, w) \models K_i\varphi$ iff $w \sim_i w'$ implies $(\mathcal{M}, w') \models \varphi$

Example [Halpern and O'Neill 2003]

$\theta(i, send(m)) \Rightarrow \neg K_j(\theta(i, send(m)))$	j does not know that i sent m
$\theta(i, send(m)) \Rightarrow \bigwedge_{k \neq j} \neg K_j(\neg\theta(k, send(m)))$	j thinks any $k \neq j$ could have

("Incomplete") Works on epistemic logic for privacy

[Halpern and O'Neill 2003] Expression of anonymity

[Tsukada et al. 2009] Expression of Anonymity, privacy, onymity, and identity

[Garcia et al. 2005] Expression of anonymity +Indistinguishability relations based on permutation equiv.

[Joinker and Pieters 2006] + Expression of receipt-freeness

[Baskar et al. 2007] Expression of vote privacy + Indistinguishability relations based on pattern matching

[Chadha et al. 2009] *Epistemic logic for the applied pi calculus* + Indistinguishability relations based on static equiv.

[van Eijck and Orzan 2007] + Tool-support – NO active attacker + NO Crypto Indistinguishability

[Boureanu et al 2009, 2010, 2012, 2016] +Tool-support – D-Y semantics "compiled" in the input to general-purpose model checkers

...

Need for tool support for verifying finer privacy specifications

Need for tool support for verifying finer privacy specifications

There are tools for verifying privacy (not expressed in epistemic logic): DEEPSEC, AKISS, diff-equivalence in Tamarin, ProVerif

BUT.....

Need for tool support for verifying finer privacy specifications

There are tools for verifying privacy (not expressed in epistemic logic): DEEPSEC, AKISS, diff-equivalence in Tamarin, ProVerif

BUT.....

Consider the "Private Authentication" Protocol [Abadi & Fournet 2004]

– S_X is a list of the public keys of X's preferred interlocutors
– Take goal 3 of this protocol, privacy of S_A: "Although an individual principal may deduce whether it is in S_A from A's willingness to communicate, A should not have to reveal anything more about S_A".

This goal is an example of privacy finesse that is not captured by any aforesaid tools!

Need for tool support for verifying finer privacy specifications

Our Work (under submission)

- a new epistemic logic that is expressive enough for privacy notions desired by the community
- a new protocol model, with an active (Dolev-Yao) attacker, to interpret this new logic
- with cryptographic indistinguishability
- an automated verification tool

Our Dolev-Yao Model for Privacy

- states == set of messages (as terms) + frame (in the applied-pi sense)
  An agent stores in its state
  - the messages $\blacksquare = \{\text{“}\textit{Hello}\text{”}, \text{alice}\}_{\text{pubk}(\textit{bob})}$
  - the frame $\{\text{“}\textit{Hello}\text{”}, \text{sender}\}_{\text{pubk}(\textit{recipient})} \mapsto \ldots.\blacksquare$
- extend Dolev-Yao deduction from messages to frames, but not just for message-deduction but also “linkability” reasoning
- build cryptographic indistinguishability over agent’s states based on pattern-matching over set of messages and over frames

Our Logics

Syntax

$$\varphi ::= has_u(\theta) \mid link_u(\tau,\theta) \mid \theta \in S_u \mid K_u\varphi \mid \neg\varphi \mid \varphi\wedge\varphi$$
$$\mid \forall x : \mathtt{D}_X \cdot \varphi \mid \forall x : Ag \cdot \varphi$$

Semantics

– standard for epistemic logic

– based primarily on crypto-based indistinguishability

– the lift is via privacy reasoning: see e.g., "link" and that $\sim$ is over states (i.e., entire frames)

1. $(M, s) \models_\alpha \neg\Phi$ iff $(M, s) \not\models_\alpha \Phi$
2. $(M, s) \models_\alpha \Phi \wedge \Psi$ iff $(M, s) \models_\alpha \Phi$ and $(M, s) \models_\alpha \Psi$
3. $(M, s) \models_\alpha has_u(\theta)$ iff $V^\alpha(\theta) \in terms(s_{V^\alpha(u)})$
4. $(M, s) \models_\alpha \theta \in S_u$ iff $V^\alpha(\theta) \in S_{V^\alpha(u)}$
5. $(M, s) \models_\alpha link_u(d, \theta)$ iff $(d \mapsto V^\alpha(\theta)) \in frame(s_{V^\alpha(u)})$
6. $(M, s) \models_\alpha K_u\varphi$ iff for all $s' \in W$ such that $s' \sim_{V^\alpha(u)} s$, $(M, s') \models_\alpha \varphi$
7. $(M, s) \models_\alpha \forall x : \mathtt{D}_X \cdot \varphi$ iff $(M, s) \models_{\alpha\cup\{x\mapsto t\}} \varphi$ for all $t \in \mathtt{D}_X$
8. $(M, s) \models_\alpha \forall x : Ag \cdot \varphi$ iff $(M, s) \models_{\alpha\cup\{x\mapsto ag\}} \varphi$

(Non-exhaustive) Flavours of Our Privacy Specifications

$$\neg(\exists x \exists a \cdot K_I(plays_x(A) \wedge named_x(a)))$$

$$\neg(\exists a \cdot K_I(\exists x \cdot plays_x(A) \wedge named_x(a)))$$

$$\neg K_I(\exists x_1, x_2 \exists a \cdot \bigwedge_{i \in \{1,2\}}(plays_{x_i}(A) \wedge named_{x_i}(a)))$$

$$\neg \exists x_1, x_2 K_I(\exists a \cdot \bigwedge_{i \in \{1,2\}}(plays_{x_i}(A) \wedge named_{x_i}(a)))$$

$$\forall x \; \forall a \; \forall b \cdot (\neg named_x(b) \wedge \neg named_x(a) \Rightarrow \neg K_x(\mathrm{pubk}(a) \notin S_b))$$

(Non-exhaustive) Flavours of Our Privacy Specifications

$\neg(\exists x \exists a \cdot K_I(plays_x(A) \wedge named_x(a)))$ (Anonymity 1)

$\neg(\exists a \cdot K_I(\exists x \cdot plays_x(A) \wedge named_x(a)))$ (Anonymity 2)

$\neg K_I(\exists x_1, x_2 \exists a \cdot \bigwedge_{i \in \{1,2\}}(plays_{x_i}(A) \wedge named_{x_i}(a)))$ (Strong Unlink)

$\neg \exists x_1, x_2 K_I(\exists a \cdot \bigwedge_{i \in \{1,2\}}(plays_{x_i}(A) \wedge named_{x_i}(a)))$ (Weak Unlink)

$\forall x\ \forall a\ \forall b \cdot (\neg named_x(b) \wedge \neg named_x(a) \Rightarrow \neg K_x(\text{pubk}(a) \notin S_b))$
(Privacy of interlocutors)

Our Model Checker for Privacy: `Phoebe`

- We built a proof-of-concept model checker for our logic and semantics, called `Phoebe`
- It generates a model for a bounded number of sessions of a protocol, and model-checks epistemic formulae of the kind shown

Protocol	Formula	$\#n_{sess}$	Domains	Time	Result
PrivAuth	Goal 3 Privacy of whitelists (who's in)	1	$D_{\mathcal{A}}$=[a,b]	46s	no attack
	Goal 3' Privacy of whitelists (who's not in)	1	$D_{\mathcal{A}}$=[a,b]	34s	no attack
	Goal 2A (Minimal) Anonymity of Initiator A	1	$D_{\mathcal{A}}$=[a,b]	109s	no attack
	Goal 2A' (Total) Anonymity of Initiator A (vs Intruder)	1	$D_{\mathcal{A}}$=[a,b]	13s	no attack
	Goal 2C (Minimal) Anonymity of Responder C	1	$D_{\mathcal{A}}$=[a,b]	99s	no attack
	Goal 2C' (Total) Anonymity of Responder C (vs Intruder)	1	$D_{\mathcal{A}}$=[a,b]	7.7s	no attack
	all goals	2	$D_{\mathcal{A}}$=[a,b]	time-out (>10h)	unknown
	all goals	1	$D_{\mathcal{A}}$=[a,b,c]	time-out (>10h)	unknown
PrivAuthX (*PrivAuth* w/o decoy messages)	Goal 3 Privacy of whitelists (who's in)	1	$D_{\mathcal{A}}$=[a,b]	0.8s	attack
	Goal 3' Privacy of whitelists (who's not in)	1	$D_{\mathcal{A}}$=[a,b]	1.44s	no attack
	Goal 2A (Minimal) Anonymity of Initiator A	1	$D_{\mathcal{A}}$=[a,b]	2.56s	no attack
	Goal 2A' (Total) Anonymity of Initiator A (vs Intruder)	1	$D_{\mathcal{A}}$=[a,b]	0.67s	no attack
	Goal 2C (Minimal) Anonymity of Responder C	1	$D_{\mathcal{A}}$=[a,b]	2.16s	attack
	Goal 2C' (Total) Anonymity of Responder C (vs Intruder)	1	$D_{\mathcal{A}}$=[a,b]	0.63s	attack
		1	$D_{\mathcal{A}}$=[a,b,c]	5.38s	attack
BasicHash	Strong Unlinkability by name	3	$D_{\mathcal{A}}$=[t1,t2,r1] ($\#n_{sess} > \#tag\_names$)	1.46s	attack
	Strong Unlinkability by name	3	$D_{\mathcal{A}}$=[t1,t2,t3,r1]	90s	no attack
`TagReader0`	Weak Unlinkability by key	2	$D_{\mathcal{A}}$=[t1,t2,r1], $D_{\mathcal{K}}$=[k1,k2]	370s	attack
	Weak Unlinkability by name	2	$D_{\mathcal{A}}$=[t1,t2,r1], $D_{\mathcal{K}}$=[k1,k2]	3h34m	no attack
	Weak Unlinkability by name	3	$D_{\mathcal{A}}$=[t1,t2,r1], $D_{\mathcal{K}}$=[k1,k2]	time-out (>10h)	unknown
`LoRaWANJoin`	Unlinkabity of DevEUI (via DevAddr)	1	$D_{\mathcal{A}}$=[d1,d2,s1]	0.39s	attack

Some Comparisons

Property	Tamarin +diff-equiv.	Proverif +diff-equiv.	DEEPSEC [2]	Phoebe
Minimal Anonymity	✓	✓	✓	✓
Total Anonymity	?	?	?	✓
Strong Unlinkability	O.A. [14]	O.A. [5]	e.g. [40]	✓
Weak Unlinkability	N/A	N/A	N/A	✓
Strong Unlinkability by key	?	O.A. [5]	?	✓
Strong Unlinkability for stateful protocols	O.A. [14]	N/A	P.	N/A
Privacy of interlocutors	N/A	N/A	N/A	✓

Future Work

- Formally characterise applied-pi restricted forms of trace equivalences via a set of epistemic formulae
- Improve our tool (e.g., on-the-fly model checking, or, narrow down the logic to fragments to which, e.g., predicate-based or agent-based abstraction, are suited)
- More case studies

Thank you!