Expressing and verifying privacy properties with epistemic logic

Fortunat Rajaona and Ioana Boureanu

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

\[ \varphi ::= p \mid \neg \varphi \mid \varphi \land \varphi \mid K_i \varphi \]

Kripke Model

\[ M = (W, \sim_i, Val) \]

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

Semantics

\[ (M, w) \models K_i \varphi \iff w \sim_i w' \text{ implies } (M, w') \models \varphi \]
Epistemic Logic: A Reminder

Syntax
\[ \varphi ::= p \mid \neg \varphi \mid \varphi \land \varphi \mid K_i \varphi \]

Kripke Model
\[ \mathcal{M} = (W, \sim_i, Val) \]
\[ W \quad \text{set of possible worlds} \]
\[ \sim_i \subseteq W \times W \quad \text{indistinguishability relations} \]
\[ Val : W \to \mathcal{P}(\mathcal{P}) \quad \text{valuation function} \]

Semantics
\[ (\mathcal{M}, w) \models K_i \varphi \text{ iff } w \sim_i w' \text{ implies } (\mathcal{M}, w') \models \varphi \]

Example [Halpern and O’Neill 2003]
\[ \theta(i, \text{send}(m)) \Rightarrow \neg K_j(\theta(i, \text{send}(m))) \quad \text{j does not know that i sent m} \]
\[ \theta(i, \text{send}(m)) \Rightarrow \bigwedge_{k \neq j} \neg K_j(\neg \theta(k, \text{send}(m))) \quad \text{j thinks any } k \neq j \text{ could have} \]
(“Incomplete”) Works on epistemic logic for privacy

[Halpern and O’Neill 2003] Expression of anonymity


[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

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
• states \(\equiv\) set of messages (as terms) + frame (in the applied-pi sense)

An agent stores in its state

- the messages \(\mathbf{\Box} = \{ "Hello", alice \}_{\text{pubk}(bob)}\)
- the frame \(\{ "Hello", \text{sender} \}_{\text{pubk}(\text{recipient})} \rightarrow \ldots \Box\)

• 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

\[ \varphi ::= \text{has}_u(\theta) \mid \text{link}_u(\tau, \theta) \mid \theta \in S_u \mid K_u \varphi \mid \neg \varphi \mid \varphi \land \varphi \]
\[ \mid \forall x : D_X \cdot \varphi \mid \forall x : Ag \cdot \varphi \]

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. \((M, s) \models_{\alpha} \Phi \land \Psi \iff (M, s) \models_{\alpha} \Phi \text{ and } (M, s) \models_{\alpha} \Psi\)
3. \((M, s) \models_{\alpha} \text{has}_u(\theta) \iff V_{\alpha}(\theta) \in \text{terms}(s_{V_{\alpha}(u)})\)
4. \((M, s) \models_{\alpha} \theta \in S_u \iff V_{\alpha}(\theta) \in S_{V_{\alpha}(u)}\)
5. \((M, s) \models_{\alpha} \text{link}_u(d, \theta) \iff (d \mapsto V_{\alpha}(\theta)) \in \text{frame}(s_{V_{\alpha}(u)})\)
6. \((M, s) \models_{\alpha} K_u \varphi \iff \text{for all } s' \in W \text{ such that } s' \sim_{V_{\alpha}(u)} s, \)
    \[ (M, s') \models_{\alpha} \varphi \]
7. \((M, s) \models_{\alpha} \forall x : D_X \cdot \varphi \iff (M, s) \models_{\alpha \cup \{x \mapsto t\}} \varphi \text{ for all } t \in D_X\)
8. \((M, s) \models_{\alpha} \forall x : Ag \cdot \varphi \iff (M, s) \models_{\alpha \cup \{x \mapsto a\}} \varphi\)
(Non-exhaustive) Flavours of Our Privacy Specifications

\neg (\exists x \exists a \cdot K_I(\text{plays}_x(A) \land \text{named}_x(a)))

\neg (\exists a \cdot K_I(\exists x \cdot \text{plays}_x(A) \land \text{named}_x(a)))

\neg K_I(\exists x_1, x_2 \exists a \cdot \land_{i \in \{1,2\}}(\text{plays}_{x_i}(A) \land \text{named}_{x_i}(a)))

\neg \exists x_1, x_2 K_I(\exists a \cdot \land_{i \in \{1,2\}}(\text{plays}_{x_i}(A) \land \text{named}_{x_i}(a)))

\forall x \forall a \forall b \cdot (\neg \text{named}_x(b) \land \neg \text{named}_x(a) \Rightarrow \neg K_x(\text{pubk}(a) \notin S_b))
(Non-exhaustive) Flavours of Our Privacy Specifications

\[ \neg (\exists x \exists a \cdot K_I(plays_x(A) \land named_x(a))) \]  
(Anonymity 1)

\[ \neg (\exists a \cdot K_I(\exists x \cdot plays_x(A) \land named_x(a))) \]  
(Anonymity 2)

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

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

\[ \forall x \forall a \forall b \cdot (\neg named_x(b) \land \neg named_x(a) \Rightarrow \neg K_x(pubk(a) \not\in S_b)) \]  
(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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Formula</th>
<th>(n_{\text{sess}})</th>
<th>Domains</th>
<th>Time</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrivAuth</td>
<td>Goal 3 Privacy of whitelists (who’s in)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>46s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 3’ Privacy of whitelists (who’s not in)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>34s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2A (Minimal) Anonymity of Initiator A</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>109s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2A’ (Total) Anonymity of Initiator A (vs Intruder)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>13s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2C (Minimal) Anonymity of Responder C</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>99s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2C’ (Total) Anonymity of Responder C (vs Intruder)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>7.7s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>all goals</td>
<td>2</td>
<td>(D_A=[a,b])</td>
<td>time-out (&gt;10h)</td>
<td>unknown</td>
</tr>
<tr>
<td></td>
<td>all goals</td>
<td>1</td>
<td>(D_A=[a,b,c])</td>
<td>time-out (&gt;10h)</td>
<td>unknown</td>
</tr>
<tr>
<td>PrivAuthX</td>
<td>Goal 3 Privacy of whitelists (who’s in)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>0.8s</td>
<td>attack</td>
</tr>
<tr>
<td></td>
<td>Goal 3’ Privacy of whitelists (who’s not in)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>1.44s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2A (Minimal) Anonymity of Initiator A</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>2.56s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2A’ (Total) Anonymity of Initiator A (vs Intruder)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>0.67s</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2C (Minimal) Anonymity of Responder C</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>2.16s</td>
<td>attack</td>
</tr>
<tr>
<td></td>
<td>Goal 2C’ (Total) Anonymity of Responder C (vs Intruder)</td>
<td>1</td>
<td>(D_A=[a,b])</td>
<td>0.63s</td>
<td>attack</td>
</tr>
<tr>
<td></td>
<td>all goals</td>
<td>2</td>
<td>(D_A=[a,b,c])</td>
<td>5.38s</td>
<td>attack</td>
</tr>
<tr>
<td>BasicHash</td>
<td>Strong Unlinkability by name</td>
<td>3</td>
<td>(D_A=[t_1,t_2,r_1]) ((#n_{\text{sess}} &gt; #\text{tag names}))</td>
<td>1.46s</td>
<td>attack</td>
</tr>
<tr>
<td></td>
<td>Strong Unlinkability by name</td>
<td>3</td>
<td>(D_A=[t_1,t_2,t_3,r_1])</td>
<td>90s</td>
<td>no attack</td>
</tr>
<tr>
<td>TagReader0</td>
<td>Weak Unlinkability by key</td>
<td>2</td>
<td>(D_A=[t_1,t_2,r_1], D_C=[k_1,k_2])</td>
<td>370s</td>
<td>attack</td>
</tr>
<tr>
<td></td>
<td>Weak Unlinkability by name</td>
<td>2</td>
<td>(D_A=[t_1,t_2,r_1], D_C=[k_1,k_2])</td>
<td>3h34m</td>
<td>no attack</td>
</tr>
<tr>
<td></td>
<td>Weak Unlinkability by name</td>
<td>3</td>
<td>(D_A=[t_1,t_2,r_1], D_C=[k_1,k_2])</td>
<td>time-out (&gt;10h)</td>
<td>unknown</td>
</tr>
<tr>
<td>LoRaWANJoin</td>
<td>Unlinkability of DevEUI (via DevAddr)</td>
<td>1</td>
<td>(D_A=[d_1,d_2,s_1])</td>
<td>0.39s</td>
<td>attack</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Minimal Anonymity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Total Anonymity</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Strong Unlinkability</td>
<td>O.A. [14]</td>
<td>O.A. [5]</td>
<td>e.g. [40]</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Weak Unlinkability</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Strong Unlinkability for stateful protocols</td>
<td>O.A. [14]</td>
<td>N/A</td>
<td>P.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Privacy of interlocutors</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
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!