A Modal Deconstruction of Access Control Logics

Universidade Federal do Rio de Janeiro

Anna Carolina C. M. de Oliveira

Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia
Programa de Engenharia de Sistemas e Computação

Tópicos Especiais em Inteligência Artificial II
November 5th 2015

Outline

Article

- Deepak Garg e Martín Abadi. **A Modal Deconstruction of Access Control.**

Introduction

- Translation from Access control logics to $S4$;
- Relying on the theory of $S4$, they obtain Kripke semantics for the logics;
- Their translation are partly based on a translation from intuitionistic logic to $S4$ that goes back to Gödel;
- *ICL* can be seen as a rather direct generalization of lax logic;
- Curry, Fairtlough and Mendler suggested interpreting lax logic in intuitionistic logic by mapping $\bigcirc s$ to $C \vee s$ or to $C \supset s$. These interpretations are sound but not complete. Compose them with a translation from intuitionistic logic to $S4$, one can map $\bigcirc s$ to $\Box((\Box C) \vee s)$ or to $\Box((\Box C) \supset s)$.

ICL

- Extends propositional intuitionistic logic with the operator **says**;
- Indexed version of *CD*, common propositional fragment of *CDD*;
- **A says** is a lax modality.

Logic

$$s ::= p \mid s_1 \wedge s_2 \mid s_1 \vee s_2 \mid s_1 \supset s_2 \mid \top \mid \bot \mid \text{A says } s$$

- Inherits all the inference rules of intuitionistic propositional logic;
- for each principal A, the formula **A says** s satisfies the following axioms:
  - $\vdash s \supset (\text{A says } s) \quad (\mathit{unit})$
  - $\vdash (\text{A says } (s \supset t)) \supset (\text{A says } s) \supset (\text{A says } t) \quad (\mathit{cuc})$
  - $\vdash (\text{A says A says } s) \supset \text{A says } s \quad (\mathit{idem})$

Example

Consider a file-access scenario with the following policy:

1. If **admin** says that **file1** should be deleted, then this must be the case.
2. **admin** trusts **Bob** to decide whether **file1** should be deleted.
3. **Bob** wants to delete **file1**.

Logical presentation:

1. (admin says $deletefile1$) $\supset$ $deletefile1$
2. admin says ((Bob says $deletefile1$) $\supset$ $deletefile1$)
3. Bob says $deletefile1$

Using (unit) and (cuc), (1)-(3) imply $deletefile1$.

ICL to $S4$

- $\ulcorner p \urcorner \; = \; \Box\, p$
- $\ulcorner s \wedge t \urcorner \; = \; \ulcorner s \urcorner \wedge \ulcorner t \urcorner$
- $\ulcorner s \vee t \urcorner \; = \; \ulcorner s \urcorner \vee \ulcorner t \urcorner$
- $\ulcorner s \supset t \urcorner \; = \; \Box\, (\ulcorner s \urcorner \supset \ulcorner t \urcorner)$
- $\ulcorner \top \urcorner \; = \; \top$
- $\ulcorner \bot \urcorner \; = \; \bot$
- $\ulcorner \mathrm{A} \text{ says } s \urcorner \; = \; \Box\, (\mathrm{A} \vee \ulcorner s \urcorner)$

Decidability

In the case of *ICL*, Theorem (soundness and completeness) implies PSPACE decidability since the same complexity bound is known for $S4$.

Kripke Model

- A Kripke model for *ICL* is a tuple $\langle W, \leq, \rho, \theta\rangle$ where
  - W is a set;
  - $\leq$ is a binary relation on W called the accessibility relation;
  - ρ is a mapping from atomic formulas of *ICL* to $\mathcal{P}(W)$ (assignment);
  - θ is a mapping from principals of *ICL* to $\mathcal{P}(W)$ (view map).

Satisfaction

- Given an *ICL* formula s and a Kripke model $\mathcal{K} = \langle W,\ \leq,\ \rho,\ \theta \rangle$, we define the satisfaction relation at a particular world ($w \vDash s$) by induction s.
  - $w \vDash p$ iff $w \in \rho(p)$
  - $w \vDash s \wedge t$ iff $w \vDash s$ and $w \vDash t$
  - $w \vDash s \vee t$ iff $w \vDash s$ or $w \vDash t$
  - $w \vDash s \supset t$ iff for each $w' \geq w,\ w' \vDash s$ implies $w' \vDash t$
  - $w \vDash \top$ for every w
  - $not(w \vDash \bot)$ for every w
  - $w \vDash \text{A says } s$ iff for every $w' \geq w$, either $w' \in \theta(\text{A})$ or $w' \vDash s$

$ICL^{\Rightarrow}$

- Extends the logic *ICL* to include a primitive "speaks for" relation ($\Rightarrow$).

Logic

- $\vdash \mathsf{A} \Rightarrow \mathsf{A} \quad (\mathit{refl})$
- $\vdash (\mathsf{A} \Rightarrow \mathsf{B}) \supset (\mathsf{B} \Rightarrow \mathsf{C}) \supset (\mathsf{A} \Rightarrow \mathsf{C}) \quad (\mathit{trans})$
- $\vdash (\mathsf{A} \Rightarrow \mathsf{B}) \supset (\mathsf{A} \text{ says } s) \supset (\mathsf{B} \text{ says } s) \quad (\mathit{speaking}-\mathit{for})$
- $\vdash (\mathsf{B} \text{ says } (\mathsf{A} \Rightarrow \mathsf{B})) \supset (\mathsf{A} \Rightarrow \mathsf{B}) \quad (\mathit{handoff})$

Example

The example was modified: instead of having **Bob** says deletefile1 directly, **Bob** delegates his authority to **Alice** (fact 3), who wants to delete **file1** (fact 4).

1. (admin says $deletefile1$) $\supset$ $deletefile1$
2. admin says ((Bob says $deletefile1$) $\supset$ $deletefile1$)
3. Bob says Alice $\Rightarrow$ Bob
4. Alice says $deletefile1$

Using (handoff) and (speaking-for), we can again derive $deletefile1$.

$ICL^{\Rightarrow}$ to $S4$

They extend to $ICL^{\Rightarrow}$ the translation from ICL to $S4$ by adding the clause:

- $\ulcorner A \Rightarrow B \urcorner = \Box (A \supset B)$

A and B are interpreted as atomic formulas in $S4$, and these atomic formulas are assumed distinct from the atomic propositions of $ICL^{\Rightarrow}$.

Decidability and Kripke Model

- Much as for *ICL*, Theorem (soundness and completeness) implies PSPACE decidability;
- Kripke models are the same as those for *ICL*;
- The satisfaction relation for $\mathrm{A} \Rightarrow \mathrm{B}$ at world w given by the clause:
  - $w \vDash \mathrm{A} \Rightarrow \mathrm{B}$ iff for every $w' \geq w,\ w' \in \theta(\mathrm{A})$ implies $w' \in \theta(\mathrm{B})$

$ICL^{\mathcal{B}}$

- Principals in ICL and $ICL^{\Rightarrow}$ are atomic and cannot be composed in logically meaningful way;
- They describe and study a systematic extension $ICL^{\mathcal{B}}$ to ICL that allows arbitrary Boolean combinations of principals with the connectives $\wedge$, $\vee$, $\supset$, $\top$, $\bot$.

Logic

$$A, B ::= a \mid A \wedge B \mid A \vee B \mid A \supset B \mid \top \mid \bot$$

- Write $\neg$ A for $(A \supset \bot)$;
- $ICL^{\mathcal{B}}$ inherits all the inference rules of *ICL*, and also includes the following additional rules:
  - $\vdash (\bot \text{ says } s) \supset s \quad (\mathit{trust})$
  - If $A \equiv \top$ then $\vdash A \text{ says } \bot \quad (\mathit{untrust})$
  - $\vdash ((A \supset B) \text{ says } s) \supset (A \text{ says } s) \supset (B \text{ says } s) \quad (\mathit{cuc}')$

Example

The following policy is analogous to that of Example in *ICL*:

1. (admin $\supset \perp$) says *deletefile*1
2. (admin says (Bob $\supset$ admin) says *deletefile*1
3. Bob says *deletefile*1

$ICL^{\mathcal{B}}$ to $S4$

The translation from ICL to $S4$ works virtually unchanged for $ICL^{\mathcal{B}}$. In the clause $\ulcorner \mathrm{A} \text{ says } s \urcorner = \Box(\mathrm{A} \vee \ulcorner s \urcorner)$, they interpret A as a formula in $S4$ in the most obvious way: each Boolean connective in A is mapped to the corresponding connective in $S4$.

Decidability

- Once more we obtain the same decidability result:

  Corollary: *There ia a polynomial space procedure that decides whether a given $ICL^{\mathcal{B}}$ formula is provable or not.*

Kripke Model

Kripke models for $ICL^{\mathcal{B}}$ may be obtained by generalizing those for ICL.

- $\hat{\theta}(a) \; = \; \theta(a)$
- $\hat{\theta}(\mathrm{A} \wedge \mathrm{B}) \; = \; \hat{\theta}(\mathrm{A}) \cap \hat{\theta}(\mathrm{B})$
- $\hat{\theta}(\mathrm{A} \vee \mathrm{B}) \; = \; \hat{\theta}(\mathrm{A}) \cup \hat{\theta}(\mathrm{B})$
- $\hat{\theta}(\mathrm{A} \supset \mathrm{B}) \; = \; (W - \hat{\theta}(\mathrm{A})) \cup \hat{\theta}(\mathrm{B})$
- $\hat{\theta}(\top) \; = \; W$
- $\hat{\theta}(\bot) \; = \; \emptyset$

From $ICL^{\Rightarrow}$ to $ICL^{\mathcal{B}}$

They prove that A $\Rightarrow$ B can be encoded as (A $\supset$ B) says $\bot$.

- $\overline{p} \ = \ p$
- $\overline{s \wedge t} \ = \ \overline{s} \wedge \overline{t}$
- $\overline{s \vee t} \ = \ \overline{s} \vee \overline{t}$
- $\overline{s \supset t} \ = \ \overline{s} \supset \overline{t}$
- $\overline{\top} \ = \ \top$
- $\overline{\bot} \ = \ \bot$
- $\overline{\mathrm{A \ says} \ s} \ = \ \mathrm{A \ says} \ \overline{s}$
- $\overline{\mathrm{A} \Rightarrow \mathrm{B}} \ = \ (\mathrm{A} \supset \mathrm{B \ says} \ \bot)$

From $ICL^{\Rightarrow}$ to $ICL^{\mathcal{B}}$

- $\vdash s$ in $ICL^{\Rightarrow}$ iff $\vdash \ulcorner s \urcorner$ in $S4$ iff $\vdash \ulcorner \overline{s} \urcorner$ in $S4$ iff $\vdash \overline{s}$ in $ICL^{\mathcal{B}}$
- $\ulcorner A \Rightarrow B \urcorner = \Box\,(A \supset B) \equiv \Box\,((A \supset B) \vee \bot) = \overline{\ulcorner A \Rightarrow B \urcorner}$

On Second-Order Quantification

- In this logic, A $\Rightarrow$ B has a well-known, compelling definition, as an abbreviation for:

$$\forall X \text{ A says } X \supset \text{B says } X$$

Logic

- The second-order logic is the straightforward extension of *ICL* with universal quantification over propositions, with the rules of System F;
- It has previously been defined and used under the name *CDD*, but they call it $ICL^{\forall}$ for the sake of uniformity;
- It immediately leads to undecidability as well as to other difficulties;
- This logic is an obvious and elegant extension of *ICL*.

Main Results

There is an obvious embedding of $ICL^{\Rightarrow}$ into $ICL^{\forall}$

- $[\![p]\!] \;=\; p$
- $[\![s \wedge t]\!] \;=\; [\![s]\!] \wedge [\![t]\!]$
- $[\![s \vee t]\!] \;=\; [\![s]\!] \vee [\![t]\!]$
- $[\![s \supset t]\!] \;=\; [\![s]\!] \supset [\![t]\!]$
- $[\![\top]\!] \;=\; \top$
- $[\![\bot]\!] \;=\; \bot$
- $[\![\mathrm{A} \text{ says } s]\!] \;=\; \mathrm{A} \text{ says } [\![s]\!]$
- $[\![\mathrm{A} \Rightarrow \mathrm{B}]\!] \;=\; \forall X\ \mathrm{A} \text{ says } X \supset \mathrm{B} \text{ says } X$

Main Results

- They define a translation from $ICL^{\forall}$ to second-order $S4$ (called $S4^{\forall}$), adding maps $\forall X \cdot s$ to $\Box\ \forall X \cdot \ulcorner s \urcorner$ in ICL translation;
- $\vdash \ulcorner [\![s]\!] \urcorner$ in $S4^{\forall}$ implies $\vdash \ulcorner s \urcorner$ in $S4$. They try to prove this by induction on s. The argument fails for a formula of the form $\mathsf{A} \Rightarrow \mathsf{B}$, since
  - $\vdash \ulcorner [\![\mathsf{A} \Rightarrow \mathsf{B}]\!] \urcorner \;=\; \Box \forall X\ \Box(\Box(\mathsf{A} \vee \Box X) \supset \Box(\mathsf{B} \vee \Box X))$
  - $\vdash \ulcorner \mathsf{A} \Rightarrow \mathsf{B} \urcorner \;=\; \Box(\mathsf{A} \supset \mathsf{B})$

Main Results

Two observations allow the proof to go through:

1. On all acyclic models, $\vdash \ulcorner [\![A \Rightarrow B]\!] \urcorner$ implies $\vdash \ulcorner A \Rightarrow B \urcorner$;

2. Quantifier-free $S4$ is sound and complete with respect to acyclic models.

Main Results

Using these observations to complete their proof as follows.

- Suppose that $\vdash [\![s]\!]$ in $ICL^{\forall}$;
- By the soundness of the translation from $ICL^{\forall}$ to $S4^{\forall}$, they obtain $\vdash \ulcorner [\![s]\!] \urcorner$ in $S4^{\forall}$;
- Therefore every acyclic model of $S4^{\forall}$ satisfies $\ulcorner [\![s]\!] \urcorner$;
- By (1), every acyclic model of $S4^{\forall}$ satisfies $\ulcorner s \urcorner$;
- Since, for $S4$ formulas, the models of $S4^{\forall}$ are the same as the models of $S4$, every acyclic model of $S4$ satisfies $\ulcorner s \urcorner$;
- By (2), every model of $S4$ satisfies $\ulcorner s \urcorner$;
- By the completeness of $S4$ for its models, it follows that $\vdash \ulcorner s \urcorner$ in $S4$;
- By soundness and completeness Theorem ($ICL^{\Rightarrow}$ to $S4$), they conclude that $\vdash s$ in $ICL^{\Rightarrow}$.

Conclusion

- Their results may serve as the basis for theorem provers for logics of access control, with the help of existing algorithms and provers for $S4$;
- The translation lead to decidability results and semantics, and also to comparison of the logics.