

A Modal Deconstruction of Access Control Logics

Deepak Garg¹ and **Martín Abadi**^{2,3}

¹Carnegie Mellon University

²University of California, Santa Cruz

³Microsoft Research

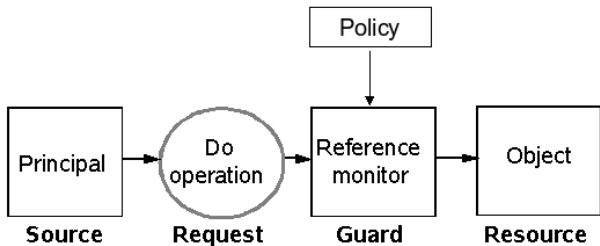
April 03, 2008

Brief Description

Study of Access Control Logics through translations to modal logic S4

- Policy
 - Rules/facts used to determine whether to allow a principal access to a resource
- Access Control Logic
 - A logic for expressing *policies* used in access control
- Principal
 - Abstraction for any entity (machine, user, program) that accesses resources or makes policies

The Problem of Access Control



- Access control is pervasive in practice, hard to get right

Logic as a Language for Policies

- Observed early on that logic is apt for expressing policies
- Policies can be expressed *naturally*
- Logic is *rigorous*
- Logic is *flexible*, and *extensible*
- First-order/propositional logic suffices
 - Exceptions: *distributed policies* and *delegation*
 - “Administrator says file1 may be deleted”
 - “Bob trusts Alice” or “Bob may represent Alice”

Access Control Logics

- Specialized logics for representing policies
- New connectives
 - A **says** s (principal A states that formula s is true)
 - $A \Rightarrow B$ (A speaks for B)

$$(A \Rightarrow B) \supset ((A \text{ says } s) \supset (B \text{ says } s))$$

- Example

- 1 (admin **says** deletefile1) \supset deletefile1
- 2 admin **says** ((Alice **says** deletefile1) \supset deletefile1)
- 3 Alice **says** (Bob \Rightarrow Alice)
- 4 Bob **says** deletefile1

Our Motivation and Results

- Many access control logics have been proposed
- Much work on representing policies, enforcement, proof-theory, languages
- Limited work in other areas
 - Decidability?
 - Kripke semantics?
 - Relating logics to each other?
- Objective of paper: fill this gap
 - Study 3 logics of access control
- Technical method: translation to well-understood logic (modal S4)
- Results:
 - Sound and complete translations to modal S4
 - Decidability, Kripke semantics
 - A complete calculus of Boolean principals
 - \Rightarrow 's encoding in second-order logic

High-Level Description

- Three logics (intuitionistic): $ICL < ICL^{\Rightarrow} < ICL^{\mathcal{B}}$
 ICL = Intuitionistic Propositional Logic + A says s
 ICL^{\Rightarrow} = $ICL + A \Rightarrow B$
 $ICL^{\mathcal{B}}$ = $ICL +$ Boolean principals

- Three translations:

$$ICL \rightarrow S4$$

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

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

- Modal logic S4 (classical)

$$\frac{\vdash s}{\vdash \Box s}$$

$$\vdash \Box s \supset s$$

$$\vdash (\Box s) \supset \Box \Box s$$

$$\vdash (\Box(s \supset t)) \supset ((\Box s) \supset (\Box t))$$

ICL: Intuitionistic Propositional Logic + A says s

- Formulas

$$s ::= p \mid s \supset t \mid s \wedge t \mid \perp \mid \dots \mid A \text{ says } s$$

- Axioms

$$\vdash s \supset A \text{ says } s$$

$$\vdash (A \text{ says } A \text{ says } s) \supset A \text{ says } s$$

$$\vdash (A \text{ says } (s \supset t)) \supset ((A \text{ says } s) \supset (A \text{ says } t))$$

All axioms of intuitionistic propositional logic

- Generalizes lax logic / CL-logic
- Prior work studies proof-theory, applications to access control

ICL \rightarrow S4

- Motivated by Gödel's translation (intuitionistic logic \rightarrow S4)

- Translation

$$\begin{aligned} \lceil p \rceil &= \Box p \\ \lceil s \supset t \rceil &= \Box(\lceil s \rceil \supset \lceil t \rceil) \\ \lceil s \wedge t \rceil &= \lceil s \rceil \wedge \lceil t \rceil \\ \lceil \perp \rceil &= \perp \end{aligned}$$

$$\lceil A \text{ says } s \rceil = \Box(A \vee \lceil s \rceil)$$

- Formula A*: "Principal *A* is unhappy."

Theorems

- Soundness and Completeness:
 $\vdash s$ in ICL if and only if $\vdash \lceil s \rceil$ in S4
- Proof based on sequent calculi
- Corollaries:
 - ICL is PSPACE decidable
 - Kripke semantics
- Special case lax logic; simplified Kripke semantics

ICL \Rightarrow : ICL + A \Rightarrow B

- Formulas:

$$s ::= \dots \mid A \Rightarrow B$$

- New Axioms:

$$\vdash (A \Rightarrow A)$$

$$\vdash (A \Rightarrow B) \supset ((B \Rightarrow C) \supset (A \Rightarrow C))$$

$$\vdash (A \Rightarrow B) \supset ((A \text{ says } s) \supset B \text{ says } s)$$

$$\vdash (A \text{ says } (B \Rightarrow A)) \supset (B \Rightarrow A)$$

- Translation:

$$\lceil A \Rightarrow B \rceil = \Box(A \supset B)$$

"If A is unhappy, so is B"

- Sound and Complete

ICL \Rightarrow is PSPACE decidable

Kripke semantics

ICL^B: ICL + Boolean principals

- Formulas same as ICL (no speaks for)
- Principals are no longer atomic

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

- View principals as Boolean algebra $\neg A = (A \supset \perp)$
- Properties of Boolean principals:

$$(A \wedge B) \text{ says } s \equiv (A \text{ says } s) \wedge (B \text{ says } s)$$

$(A \vee B) \text{ says } s$: Statements of A and B together imply s

$(A \supset B) \text{ says } s$: A speaks for B on s and its consequences

$$A \Rightarrow B \text{ may be defined as } (A \supset B) \text{ says } \perp$$

$\top \text{ says } s$: Always (\top is a liar)

$$(\perp \text{ says } s) \supset s$$

- Translation to S4: same as that from ICL

ICL^B is PSPACE decidable

Kripke semantics

Translations from ICL^{\Rightarrow}

- Intuitive embedding from $ICL^{\Rightarrow} \rightarrow ICL^{\mathcal{B}}$
 $A \Rightarrow B \longrightarrow (A \supset B)$ **says** \perp
- Embedding is sound and complete
 $ICL^{\mathcal{B}}$ is more expressive than ICL^{\Rightarrow}
- Another embedding from $ICL^{\Rightarrow} \rightarrow ICL + \text{Second order } \forall$
 $A \Rightarrow B \longrightarrow \forall X. (A \text{ **says** } X) \supset (B \text{ **says** } X)$
- Soundness straightforward: verify axioms
- Completeness non-intuitive
 Proof uses non-standard detour in Kripke semantics

Summary and Future Work

- Summary

- Translation from access control logics to S4 gives decidability, Kripke semantics
- Description of Boolean principals
- Interpretation of \Rightarrow using second order \forall

- Future Work

- Other access control logics
- Theorem proving using translations

Proof of embedding $ICL^{\Rightarrow} \rightarrow ICL^B$

- $A \Rightarrow B \longrightarrow (A \supset B)$ says \perp

$$\begin{aligned}
 \vdash A \Rightarrow B &\leftrightarrow \vdash \Box(A \supset B) \\
 &\equiv \vdash \Box((A \supset B) \vee \perp) \\
 &\leftrightarrow \vdash (A \supset B) \text{ says } \perp
 \end{aligned}$$

Kripke Semantics for ICL

- Take standard models for intuitionistic propositional logic
 - W is a set of worlds
 - \leq accessibility relation (pre-order)
 - $\rho : (\text{Atomic formulas}) \rightarrow \mathcal{P}(W)$
- Add a “happiness function”, $\theta : \text{Principals} \rightarrow \mathcal{P}(W)$
 - $w \in \theta(A) \iff A$ is unhappy in world w
- $w \models A$ **says** s if and only if for each $w' \geq w$, $w' \in \theta(A)$ or $w' \models A$

Kripke Semantics for Lax Logic

- Take standard models for intuitionistic propositional logic
 - W is a set of worlds
 - \leq accessibility relation (pre-order)
 - $\rho : (\text{Atomic formulas}) \rightarrow \mathcal{P}(W)$
- Classify worlds into “good” and “bad”
- $w \models \bigcirc s$ if and only if for each $w' \geq w$, w' is bad or $w' \models A$

Comparison to Mendler's Translation

- Mendler's translation composed with Gödel's translation:

$$\ulcorner \Box s \urcorner = \Box((\Box A) \vee \ulcorner s \urcorner)$$

- Our translation

$$\ulcorner \Box s \urcorner = \Box(A \vee \ulcorner s \urcorner)$$