# Modal Access Control Logic

**Axiomatization, Semantics and FOL Theorem Proving**

**Valerio Genovese**[1] and **Daniele Rispoli** [2] and **Dov M. Gabbay** [3] and **Leendert van der Torre** [4]

**Abstract.** We present and study a Modal Access Control Logic (M-ACL) to specify and reason about access control policies. We identify canonical properties of well-known access control axioms. We provide a Hilbert-style proof-system and we prove soundness, completeness and decidability of the logic. We present a sound and complete embedding of Modal Access Control Logic into First-Order Logic. We show how to use SPASS theorem prover to reason about access control policies expressed as formulas of Modal Access Control Logic, and we compare our logic with existing ones.

## 1 Introduction

Access control is concerned with the decision when to accept or deny a request from a principal (e.g., user, program) to do an operation on an object. In practice, an access control system is a product of several, often independent, distributed entities with different policies that interact in order to determine access to resources. In order to specify and reason about such systems, many formal frameworks have been proposed [10, 13, 14]

A common feature of almost all well-known approaches is the employment of formulas of the form "$K$ says $\varphi$", intuitively meaning that principal $K$ *asserts* or *supports* $\varphi$ to hold in the system. On top of the says operator many other constructs have been proposed, a central one is the speaks-for relationship to model delegation between principals. More precisely, we say that a principal "$K$ speaks-for $K'$" if $K$ says $\varphi$ implies that also $K'$ says $\varphi$.

Recently the increasing need to evaluate, combine and integrate different access control architectures motivated researchers to study logics themselves [1, 8, 9, 10]. This research trend shifted the attention from ad-hoc formalisms to the identification of common foundations for access control logics by studying their formal, mainly unexplored, properties (e.g., axiomatizations, expressiveness, decidability and semantics). Even if there is some agreement on looking at the says construct as a *modal* operator, the correspondence theory between its axiomatizations and the underlying (Kripke-style) semantics is often left unexplored.

In this paper we address the following research question: *can Kripke semantics be employed to specify and reason about access control policies?* This breaks down in two sub-questions:

*- what is a sound and complete axiomatization of well-known access control axioms with respect to a Kripke semantics?*

*- how can Kripke semantics be used to employ state-of-the-art theorem provers to reason about policies?*

These questions raise several challenges. First of all, axioms of access control are not standard in modal literature and their correspondence with the underlying semantics is mainly unexplored. Identifying canonical properties for well-known axioms for access control permits to study them separately and naturally yields completeness for logics that adopt *any* combination of them. This approach is significant if we want logic to be employed to compare different access control models, because different systems adopt different axioms depending on the specific application domain.

Moreover, one emergent trend is the use of intuitionistic logics for authorization (see Section 7), therefore we need to concentrate on a new *constructive* modal logic. In order to directly employ semantics in the reasoning process we present an embedding of our logic into First-Order Logic (FOL) and then we show how to use a theorem prover to carry out sound and complete deductions.

In this paper we present a novel intuitionistic access control logic called Modal Access Control Logic (M-ACL), we establish a tight correspondence between axioms of the logic and semantics (via soundness and completeness proofs), we exploit this correspondence by relying on the semantics to embed M-ACL into FOL, we prove decidability and then we show how to employ SPASS theorem prover to reason about access control policies expressed in M-ACL.

The paper is structured as follows: Section 2 presents the syntax and axiomatization of M-ACL. Section 3 introduces the constructive semantics while Section 4 and 5 are devoted to prove completeness and decidability, respectively. Section 6 presents the parser from M-ACL syntax into First Order Logic and how to use the translation to reason with SPASS theorem prover. Section 7 underlines related work and Section 8 ends the paper with conclusions and future work.

## 2 Modal Access Control Logic

M-ACL is an access control logic based on intuitionistic multi-modal logic which extends intuitionistic propositional logic with two operators:

- A binary modality $\Box_K$ indexed by a principal, where $\Box_K\varphi$ has to be read as "$K$ says $\varphi$".
- A binary operator between principals $\Rightarrow$, were $K \Rightarrow K'$ stands for "$K$ speaks-for $K'$".

**Definition 1 (M-ACL syntax)** *Formulae of M-ACL are defined by the following grammar*

$$\varphi ::= p \mid \bot \mid \neg\varphi \mid (\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \rightarrow \varphi) \mid (K \Rightarrow K') \mid \Box_K\varphi$$

*where,*

- *$p$ ranges over a set of Boolean variables $\Phi_0$,*
- *$K$ and $K'$ range over a set of principals $\mathcal{P}$.*

[1] University of Luxembourg, Luxembourg, and University of Torino, Italy, valerio.genovese@uni.lu
[2] Independent researcher, daniele.rispoli@gmail.com
[3] King's College, London, dov.gabbay@kcl.ac.uk
[4] University of Luxembourg, Luxembourg, leendert@vandertorre.com

**Definition 2 (M-ACL Axiomatization)** *The axiomatization of M-ACL consists of all axioms of intuitionistic propositional logic plus axioms and rules for the says ($\Box$) and speaks-for ($\Rightarrow$) operators.*

| | |
|---|---|
| *all axioms of intuitionistic propositional logic* | *(IPC)* |
| *If* $\vdash \varphi$ *then* $\vdash \Box_K \varphi$ | *(N)* |
| *If* $\vdash \varphi$ *and* $\vdash \varphi \to \psi$, *then* $\vdash \psi$ | *(MP)* |
| $\vdash \Box_K(\varphi \to \psi) \to \Box_K \varphi \to \Box_K \psi$ | *(K)* |
| $\vdash \varphi \to \Box_K \varphi$ | *(Unit)* |
| $\vdash \Box_K(\Box_K \varphi \to \varphi)$ | *(C)* |
| $\vdash K \Rightarrow K$ | *(S-refl)* |
| $\vdash (K \Rightarrow K') \to (K' \Rightarrow K'') \to (K \Rightarrow K'')$ | *(S-trans)* |
| $\vdash K \Rightarrow K' \to \Box_K \varphi \to \Box_{K'} \varphi$ | *(speaking-for)* |
| $\vdash \Box_{K'}(K \Rightarrow K') \to (K \Rightarrow K')$ | *(handoff)* |

(N) and (K) are standard for normal modal logics, (Unit) is a well known axiom in access control and states that for every formula $\varphi$, if it holds, then it is supported by every principal $K$. (C) has been employed in authorization logics [8] and comes from doxastic logic. Intuitively, (C) means that every principal says that all its statements have to hold. (S-refl),(S-trans) and (speaking-for) come from [9] and model the speaks-for relationship. (handoff) states that whenever $K'$ says that $K$ speaks-for $K'$, then $K$ does indeed speak for $K'$ (i.e., every principal can decide which principals speak on its behalf).

The above axioms are not new in the access control literature and, as shown in [8], most of the logic-based security policy systems are based on (a subset of) them. However, M-ACL is the first access control logic that combines them in a unique system, for this reason it can be seen as a generalization of both logics presented in [9] and [8].

**Theorem 1 (Deduction Theorem for M-ACL)** *Given two wff $\varphi$ and $\psi$*

$$\varphi \vdash \psi \text{ implies } \vdash \varphi \to \psi$$

*where $\varphi \vdash \psi$ means that assuming $\varphi$ we can derive (in the axiomatic proof-system of Definition 2) $\psi$.*

**Proof.** This theorem follows from the deduction theorem of intuitionistic propositional logic (IPC) and the fact that M-ACL is an axiomatic extension of IPC. □

We conclude this section by providing a simple example of how policies can be represented in M-ACL

**Example 1 (Taken literally from [9])** *Consider the following scenario with three principals* `Admin`, `Bob`, `Alice` *and one file (*`file1`*) together with the following policy:*

*(1)* *If the administrator (*`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` *delegates its authority to* `Alice`.
*(4)* `Alice` *wants to delete* `file1`.

*The policy can be encoded in M-ACL*[5] *as follows:*

*(1)* `admin` *says* `delete_file1` $\to$ `delete_file1`
*(2)* `admin` *says (*(`Bob` *says* `delete_file1`*)* $\to$ `delete_file1`*)*
*(3)* `Bob` *says (*`Alice` $\Rightarrow$ `Bob`*)*
*(4)* `Alice` *says* `delete_file1`

*The question of whether* `file1` *should be deleted corresponds to prove* `delete_file1`*, which follows from (2)-(4),(Unit),(K),(handoff) and (speaking-for).*

[5] For the sake of readability we write "$A$ says $\varphi$" instead of "$\Box_A \varphi$".

## 3 M-ACL Constructive Semantics

Semantics for M-ACL is based on standard semantics for constructive modal logic, defined as follows

**Definition 3** *An intuitionistic model $\mathcal{M}$ for M-ACL is a tuple $(S, \leq, \{R_K\}_{K \in \mathcal{P}}, h)$ where*

- *$(S, \leq)$ is a preordered set.*
- *$R_K$ is a binary relation on $S$.*
- *$h$ is an assignment which, for each boolean variable $q$, assigns the subset of worlds $h(q) \subseteq S$ where $q$ holds. Moreover, we require $h$ to be monotone w.r.t $\leq$ i.e., $x \in h(q)$ and $x \leq y$ then $y \in h(q)$.*

An *interpretation* for the logic is a pair $\mathcal{M}, t$ where $\mathcal{M}$ is a model and $t$ a state (or world) in $\mathcal{M}$. The satisfaction relation "$\models$" holds between interpretations and formulae of the logic, and it is defined as follows (we omit $\wedge$ and $\vee$):

- $\mathcal{M}, t \models q$ iff $t \in h(q)$
- $\mathcal{M}, t \not\models \bot$
- $\mathcal{M}, t \models \varphi \to \psi$ iff for all $s, t \leq s$ and $\mathcal{M}, s \models \varphi$ implies $\mathcal{M}, s \models \psi$
- $\mathcal{M}, t \models \neg\varphi$ iff for all $s$, $t \leq s$ implies $\mathcal{M}, s \not\models \varphi$
- $\mathcal{M}, t \models K' \Rightarrow K$ iff for all $s$, $tR_K s$ implies $tR_{K'} s$
- $\mathcal{M}, t \models \Box_K \psi$ iff for all $s$ such that $tR_K s$ we have $\mathcal{M}, s \models \psi$

Moreover, we force all models $\mathcal{M}$ of M-ACL to satisfy the semantical conditions reported in Definition 4.

**Definition 4 (Semantical Conditions)** *For any two principals $K$ and $K'$, we impose on $\leq$, $R_K$ and $R_{K'}$ the following conditions to hold:*

*(a)* $\forall x, y((xR_K y \to xR_{K'} y) \to (\forall s, z(x \leq s \to (sR_K z \to sR_{K'} z))))$
*(b)* $\forall x, y, z((x \leq y \wedge yR_K z) \to xR_K z)$
*(c)* $\forall x, y(xR_K y \to x \leq y)$
*(d)* $\forall x, y(xR_K y \to yR_K y)$
*(e)* $\forall x, y((xR_K y \to \forall z(yR_K z \to yR_{K'} z)) \to \forall s(xR_K s \to xR_{K'} s))$

Conditions (a) and (b) ensure monotonicity for speaks-for and modal formulas (see Lemma 1), conditions (c), (d) and (e) are the semantic conditions associated with axiom (Unit), (C) and (handoff) respectively. In Section 4 we show that each condition is canonical for the corresponding axiom, i.e., it is *necessary* and *sufficient* for the corresponding axiom to hold.

We now show that condition $(e)$ is implied by conditions $(b)$, $(c)$ and $(d)$, but we prefer to make it explicit. In fact, having canonical conditions for each of the axioms permits to study them separately from each other and naturally yields completeness for logics which adopt *any* combination of them. For instance, $Unit$ is a strong axiom adopted in both [9, 8], but not every access control system implements it. With our methodology we can provide soundness and completeness for a weaker logic without $Unit$ by removing the corresponding axiom from Definition 2 and condition (c) from Definition 4.

**Observation 1** *The semantical condition corresponding to (hand-off) is implied by conditions* $(b)$, $(c)$ *and* $(d)$ *in Definition 4.*

**Proof.** Given a model $\mathcal{M}$, suppose we are in a world $x$ in which the antecedent of $(e)$ holds i.e., $\mathcal{M}, x \models \Box_K(K' \Rightarrow K)$ and suppose, for the sake of contradiction, that the consequent does not hold. Then, there is a world $s$ such that $xR_Ks$ and $\neg(xR_{K'}s)$. By hypothesis and with condition $(d)$ we have that for every $R_K$ accessible world $y$ from $x$, $yR_Ky$ and $yR_{K'}y$. But then, by conditions $(b)$ and $(c)$ we have that for any world $y$, $xR_Ky$ implies $xR_{K'}y$, so it must be $xR_{K'}s$, which is a contradiction. □

**Lemma 1 (Monotonicity)** *For any wff* $\varphi$ *and an interpretation* $\mathcal{M}, t$*, such that* $\mathcal{M}$ *satisfies semantical conditions of Definition 4 we have that, if* $\mathcal{M}, t \models \varphi$ *and* $t \leq s$ *then* $\mathcal{M}, s \models \varphi$

**Proof.** By structural induction on $\varphi$, we show the modal case:

($\varphi = \Box_K\psi$), suppose $\mathcal{M}, t \models \Box_K\psi$, we want to show that for any s, such that $t \leq s$ we have $\mathcal{M}, s \models \Box_K \psi$. By contradiction suppose that there exists a state t', such that $s \leq t'$ and $\mathcal{M}, t' \not\models \Box_K \psi$. Then it exists a world $r$ K-accessible from $t'$ (i.e., $t'R_Kr$) such that $\mathcal{M}, r \not\models \psi$, but by condition (b) we have also that $sR_Kr$ so, by hypothesis $\mathcal{M}, r \models \psi$, which is a contradiction. □

**Theorem 2 (Soundness for M-ACL)** *If* $\vdash \varphi$ *then* $\models \varphi$.

**Proof.** By structural induction on $\varphi$. □

## 4 Completeness

**Definition 5 (Consistency)** $\Gamma$ *is consistent iff* $\Gamma \nvdash \bot$. *If* $\Gamma$ *has an infinite number of formulas, we say that* $\Gamma$ *is consistent iff there are no finite* $\Gamma_0 \subset \Gamma$ *such that* $\Gamma_0 \vdash \bot$.

**Definition 6 (Saturation)** *Let* $\Gamma$ *be a set of well formed formulas, we say that* $\Gamma$ *is saturated iff*

1. $\Gamma$ *is consistent,*
2. *For all principals* $K, K'$ *either* $(K \Rightarrow K') \in \Gamma$ *or* $\neg(K \Rightarrow K') \in \Gamma$
3. *If* $\Gamma \vdash \varphi$ *then* $\varphi \in \Gamma$
4. *If* $\Gamma \vdash \varphi \vee \psi$ *then* $\Gamma \vdash \varphi$ *or* $\Gamma \vdash \psi$

**Lemma 2 (Saturated Extensions)** *Suppose* $\Gamma \nvdash A$*, there is a saturated extension* $\Gamma^*$ *such that* $\Gamma^* \nvdash A$.

**Proof.** This is proved by standard Lindenbaum construction. We obtain $\Gamma^*$ as $\bigcup\{\Gamma^k : k \in \mathcal{N}\}$, with $\Gamma_0 = \Gamma \cup \{\neg A\}$, $\Gamma^k \backslash \Gamma$ is finite. We now provide an inductive definition of $\Gamma^{k+1}$. Let $\{\beta_1, \ldots \beta_n, \ldots\}$ be an enumeration of formulas of M-ACL and define $\Gamma^{k+1}$ to be

- $\Gamma^k$ if $\Gamma^k \cup \beta_i$ is inconsistent
- $\Gamma^k \cup \beta_i$ otherwise

We now prove that $\Gamma^* \nvdash A$. Suppose that $\Gamma^* \vdash A$, then $\Gamma^*$ is inconsistent since $\neg A \in \Gamma_0$, hence $\neg A \in \Gamma^*$. Now, at every stage $\Gamma_k$ is, by construction, consistent and by compactness, if $\Gamma^*$ is inconsistent then some finite subset is inconsistent, which means that some $\Gamma_k$ is inconsistent, which is a contradiction. □

**Lemma 3** *Let* $\Gamma$ *be a set of formulas and let* $\Delta = \{\alpha : \Box_K\alpha \in \Gamma\}$. *If* $\Delta \vdash \beta$*, then* $\Gamma \vdash \Box_K\beta$

**Proof.** Suppose there is a derivation of $\beta$ from $\Delta$. Then, there must be a finite set of formulas $\{\alpha_1, \ldots, \alpha_n\} \subseteq \Delta$ such that $\{\alpha_1, \ldots, \alpha_n\} \vdash \beta$. By Theorem 1, $\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \rightarrow \beta$. By (N) and (K), $\vdash \Box_K\alpha_1 \wedge \ldots \wedge \Box_K\alpha_n \rightarrow \Box_K\beta$. As $\Box_K\alpha_i \in \Gamma$ for all $i = 1, n$, by modus ponens, $\Gamma \vdash \Box_K\beta$. □

**Definition 7 (Canonical model construction)** *Let* $\Gamma_0$ *be any theory (set of formulas). Then we define* $\mathcal{M}^* = (S, \leq, \{R_K\}_{K \in \mathcal{P}}, h)$, *where*

- $S$ *is the set of all saturated* $\Gamma \supset \Gamma_0$.
- $\Gamma_1 \leq \Gamma_2$ *iff* $\Gamma_1 \subseteq \Gamma_2$.
- $\Gamma_1 R_K \Gamma_2$ *iff* $\{\alpha \mid \Box_K\alpha \in \Gamma_1\} \subseteq \Gamma_2$
- $\Gamma \in h(q)$ *iff* $q \in \Gamma$

**Lemma 4** *For all* $\Gamma \in S$ *and each wff formula* $\varphi$

$$\Gamma \models \varphi \Leftrightarrow \varphi \in \Gamma$$

**Proof.** By induction on the complexity of $\varphi$, we look at some cases

- *Case 1.*: For $\varphi$ atomic the lemma holds by definition.
- *Case 2.*: Let $\varphi \equiv \Box_K\beta$ , and suppose $\Gamma \models \Box_K\beta$. Hence, for all $\Gamma'$ such that $\Gamma R_K \Gamma'$, $\Gamma' \models \beta$ By inductive hypothesis, $\beta \in \Gamma'$, let $\Delta = \{\alpha : \Box_K\alpha \in \Gamma\}$. By construction, $\Gamma' \supseteq \Delta$. Assume, by absurdum, that $\Box_K\beta \notin \Gamma$. By the saturation condition (2), $\Gamma \nvdash \Box_K\beta$. Then, by Lemma 3, $\Delta \nvdash \beta$. By Lemma 2, there is a saturated extension $\Delta^*$ such that $\Delta^* \nvdash \beta$. This contradicts the fact that, for all $\Gamma'$ such that $\Gamma R_K \Gamma'$, $\beta \in \Gamma'$, i.e., that (by construction of the canonical model) for all saturated sets $\Gamma'$ such that $\Gamma' \supseteq \Delta$, $B \in \Gamma'$. The converse is trivial.
- *Case 3.*: Let $\varphi \equiv K \Rightarrow K'$, it then follows from Definition 6 that $K \Rightarrow K' \in \Gamma$

□

To show that the canonical model $\mathcal{M}^*$ defined above is indeed a model of M-ACL, we have to prove that it satisfies the conditions in Definition 4.

**Lemma 5** *Let* $\mathcal{M}^*$ *be the canonical model as defined in Definition 7.* $\mathcal{M}^*$ *satisfies conditions (a), (b), (c), (d) and (e) of Definition 4.*

**Proof.** We have to prove that

(a) $\forall\Gamma_1, \Gamma_2((\Gamma_1 R_K \Gamma_2 \rightarrow \Gamma_1 R_{K'} \Gamma_2) \rightarrow (\forall\Gamma_3, \Gamma_4(\Gamma_1 \leq \Gamma_3 \rightarrow (\Gamma_3 R_K \Gamma_4 \rightarrow \Gamma_3 R_{K'} \Gamma_4))))$
(b) $\forall\Gamma, \Gamma', \Gamma'' \in S$, if $\Gamma \leq \Gamma'$ and $\Gamma' R_K \Gamma''$ then $\Gamma R_K \Gamma''$
(c) $\forall\Gamma, \Gamma' \in S$, if $\Gamma R_K \Gamma'$ then $\Gamma \leq \Gamma'$
(d) $\forall\Gamma, \Gamma' \in S$, if $\Gamma R_K \Gamma'$ then $\Gamma' R_K \Gamma'$
(e) $\forall\Gamma_1, \Gamma_2((\Gamma_1 R_K \Gamma_2 \rightarrow \forall\Gamma_3(\Gamma_2 R_K \Gamma_3 \rightarrow \Gamma_2 R_{K'} \Gamma_3)) \rightarrow \forall\Gamma_4(\Gamma_1 R_K \Gamma_4 \rightarrow \Gamma_1 R_{K'} \Gamma_4))$

The proof of points (a) and (b) is trivial and follows from that for any two worlds $\Gamma_1, \Gamma_2$, if $\Gamma_1 \leq \Gamma_2$ then $\Gamma_1 \subseteq \Gamma_2$.

Let us prove point (c). We want to show that if $\Gamma R_K \Gamma'$ then $\Gamma \leq \Gamma'$. Take a world $\Delta \in S$, for any formula $\varphi \in \Delta$ we have that $\Box_K\varphi \in \Delta$ (by Unit and MP) which means that for every $\Delta'$ such that $\Delta R_K \Delta'$ $\varphi \in \Delta'$, which means that $\Delta \leq \Delta'$.

Relating point (d) we have to show that if $\Gamma R_K \Gamma'$ then $\Gamma' R_K \Gamma'$. Take a world $\Delta \in S$, for any formula $\varphi$ we have that $\Box_K(\Box_K\varphi \rightarrow \varphi) \in \Delta$ (by C), so for any world $\Delta' \in S$ such that $\Delta R_K \Delta'$ and $(\Box_K\varphi \rightarrow \varphi) \in \Delta'$, we have to show that $\Delta' R_K \Delta'$. By definition of $R_K$ in the canonical model, this means that we must prove that if

$\Box_K\varphi \in \Delta'$ then $\varphi$, but this follows from $\Box_K\varphi \to \varphi \in \Delta'$, so we are done.

Concerning point (e) we have to show that, for any world $\Gamma \in S$ if $\Gamma \models \Box_K(K' \Rightarrow K)$ then $\Gamma \models K' \Rightarrow K$. This follows from the fact that, by (handoff), $(\Box_K(K' \Rightarrow K) \to K' \Rightarrow K) \in \Gamma$ and that $\Gamma$ is saturated. □

**Theorem 3 (Strong completeness for M-ACL)** *If $\Gamma \models \varphi$ then $\Gamma \vdash \varphi$*

**Proof.** Suppose $\Gamma \nvdash \varphi$, and let $\Gamma_0$ be a saturated extension of $\Gamma$, $\varphi \notin \Gamma_0$; construct a canonical model $\mathcal{M}^*$ as in Definition 7, then $\mathcal{M}^*, \Gamma_0 \not\models \varphi$. This yields completeness. □

## 5 Decidability

In this section we prove decidability of M-ACL using a technique introduced in [2] which generalizes a decidability result reported in [7]. Following [2] we first show that M-ACL semantics can be embedded into a monadic two-variable guarded fragment ($GF^2_{mon}$) of classical first-order logic, and then we show that M-ACL identifies a class $\mathcal{C}$ of Kripke models defined by an acyclic set of monadic second-order (MSO) definable closure conditions on relations $\leq$ and $\{R_K\}_{K\in\mathcal{P}}$.

We start by defining $GF^2_{mon}$. In the following $FV(\varphi)$ stands for the set of free variables of $\varphi$, and $\overline{x}$ stands for a sequence of variables. We assume a first order language which contains predicate letters of arbitrary arity, including equality, and no constants or functional symbols.

**Definition 8** *The guarded fragment $GF$ of first-order logic is the smallest set containing all first-order atoms, closed under boolean connectives and the following rule: if $\rho$ is an atom, $\varphi \in GF$, and $\overline{x} \subseteq FV(\varphi) \subseteq FV(\rho)$, then $\exists\overline{x}(\rho \wedge \varphi)$ and $\forall\overline{x}(\rho \to \varphi) \in GF$ (in such a case $\rho$ is called a guard).*

**Definition 9** *The monadic two-variable guarded fragment $GF^2_{mon}$ is a subset of $GF$ containing formulas $\varphi$ such that (i) $\varphi$ has no more than two variables (free or bound), and (ii) all non-unary predicate letters of $\varphi$ occur in guards.*

Now we show that M-ACL semantics can be translated into $GF^2_{mon}$. In line with [2] we define, by mutual recursion, two translations, $\tau_x$ and $\tau_y$, so that a first-order formula $\tau_v(\varphi)$ ($v \in \{x, y\}$) contains a single free variable $v$, which intuitively stands for the world at which $\varphi$ is being evaluated in the Kripke model.

**Definition 10 (M-ACL embedding into $GF^2_{mon}$)** *We define $\tau_x(\varphi)$[6] by structural induction on the complexity of $\varphi$*

- $\tau_x(p) = P(x)$
- $\tau_x(\neg\varphi) = \forall y(x \leq y \to \neg\tau_y(\varphi))$
- $\tau_x(\varphi \wedge \psi) = \tau_x(\varphi) \wedge \tau_x(\psi)$
- $\tau_x(\varphi \vee \psi) = \tau_x(\varphi) \vee \tau_x(\psi)$
- $\tau_x(\varphi \to \psi) = \forall y(x \leq y \to \neg\tau_y(\varphi) \vee \tau_y(\psi))$
- $\tau_x(K \Rightarrow K') = \forall y(x \leq y \to \forall x(yR_{K'}x \to yR_Kx))$
- $\tau_x(\Box_K\varphi) = \forall y(x \leq y \to \forall x(yR_Kx \to \tau_x(\varphi))$

*The translation of the modality and speaks for (i.e., $\tau_x(\Box_K\varphi)$ and $\tau_x(K \Rightarrow K')$) forces directly monotonicity of $\Box$ and $\Rightarrow$. It is equivalent (in the sense of Theorem 4) to the definition of $\mathcal{M}, x \models K \Rightarrow K'$ and $\mathcal{M}, x \models \Box_K\varphi$ satisfying respectively conditions (a) and (b) of Definition 4.*

[6] $\tau_y$ is defined analogously, switching the roles of $x$ and $y$.

**Theorem 4** *Let $\varphi$ be a M-ACL formula and $\mathcal{C}$ be a class of models of M-ACL. Let $\mathcal{M} \in \mathcal{C}$. Then, $\mathcal{M}, w \models \varphi$ iff $\mathcal{M} \models \tau_x(\varphi)[x/w]$*[7].

**Proof.** By structural induction of $\varphi$. □

**Definition 11** *Let $W$ be a non-empty set. A unary function $C$ on the powerset of $W^n$ is a **closure operator** if, for all $\mathcal{P}, \mathcal{P}' \subseteq W^n$,*

1. *$\mathcal{P} \subseteq C(\mathcal{P})$ (C is increasing)*
2. *$\mathcal{P} \subseteq \mathcal{P}'$ implies $C(\mathcal{P}) \subseteq C(\mathcal{P}')$ (C is monotone)*
3. *$C(\mathcal{P}) = C(C(\mathcal{P}))$ (C is idempotent)*

*An $m+1$-ary function $C$ on the powerset of $W^n$ is a **parametrised closure operator** if, given any choice of $m$ relations $\mathcal{P}_1, \ldots, \mathcal{P}_m \subseteq W^n$, it gives rise to a unary function $C^{\mathcal{P}_1,\ldots\mathcal{P}_m}$ (parametrised by $\mathcal{P}_1, \ldots, \mathcal{P}_m$) that is a simple closure operator on the powerset of $W^n$*

In order to characterize M-ACL models we need the following closure operators[8]: A reflexive and transitive closure operator $TC(\mathcal{P})$; A parametrized inclusion operator $Incl^{\mathcal{P}'}(\mathcal{P}) = \mathcal{P}' \cup \mathcal{P}$; A one step reflexivity operator $1SR(\mathcal{P})$;

**Definition 12** *A condition on relation $\mathcal{P}$ is a **closure condition** if it can be expressed in the form $C(\mathcal{P}) = \mathcal{P}$, where $C$ is a closure operator.*

The following are the closure conditions for relations $\leq$ and $\{R_K\}_{K\in\mathcal{P}}$ of M-ACL: $TC(\leq) = \leq$ (reflexivity-and-transitivity closure condition); $Incl^{R_K}(\leq) = \leq$ ($R_K$ is subset of $\leq$); $1SR(R_K) = R_K$ (one-step-reflexivity closure condition).

**Definition 13** *Let $S$ be a set of relations and $\mathbf{C}$ a set of closure conditions on relations in $S$. Let us say for $\mathcal{P}, \mathcal{P}' \in S$, that $\mathcal{P}$ depends on $\mathcal{P}'$ if $\mathbf{C}$ contains a parametrised condition of the form $C^{\mathcal{P}_1,\ldots,\mathcal{P}',\ldots,\mathcal{P}_m}(\mathcal{P}) = \mathcal{P}$. A set of closure conditions $\mathbf{C}$ is **acyclic**, if its "depends on" relation is acyclic.*

**Theorem 5 (proof in [2])** *Let $\mathbf{M}$ be a class of intuitionistic modal models defined by an acyclic set of MSO closure conditions on its relations (e.g. $\leq$, accessibility modal relations,...) so that at most one closure condition is associated with each relation, and let $\varphi$ be an intuitionistic modal formula. Then, it is decidable whether $\varphi$ is satisfiable in $\mathcal{M}$.*

Now, on the basis of 5 we show that all the conditions reported above can be expressed in Monadic Second-Order Logic.

**Definition 14** *The closure operators of M-ACL can be represented in Monadic Second-Order Logic as follows:*

- *Closure operator $TC$ is definable by the MSO formula $TC_{\leq}(z_1, z_2) = \forall X(X(z_1) \wedge \forall x, y(X(x) \wedge x \leq y \to X(y)) \to X(z_2))$*
- *Closure operator $Incl^{R_K}(\leq)$ is definable by the MSO formula: $Incl^{\leq}_{R_K}(z_1, z_2) = R_K(z_1, z_2) \vee z_1 \leq z_2$*
- *The one-step reflexivity operator $1SR(R_K)$: $1SR_{R_K}(z_1, z_2) = R_K(z_1, z_2) \vee \exists x(R_K(x, z_1) \wedge z_1 = z_2)$*

**Theorem 6 (M-ACL Decidability)** *M-ACL is decidable*

[7] Where $\mathcal{M}$ is taken as a model of first order logic with relations $\leq$ and $\{R_K\}_{K\in\mathcal{P}}$ respecting properties of M-ACL semantics, and $\varphi[x/w]$ is the result of substituting $w$ for the free variable $x$.

[8] The formal specification of these operators is given in Definition 14.

**Proof.** M-ACL is an intuitionistic modal logic with indexed modalities $\Box_K$, defined by the class of models where the following closure conditions on $R_K$ (for each $K \in \mathcal{P}$) and $\leq$ are specified: $TC(\leq) = \leq; Incl^{R_K}(\leq) = \leq; 1SR(R_K) = R_K$. This set of conditions is acyclic and each condition is MSO definable. However there are two constraints associated with $\leq$. To satisfy the conditions of Theorem 5 we need to combine them into one MSO definable closure condition. Alechina et al. report in [2] that $TC \circ Incl^{\mathcal{P}'}$ is a closure operator with the property that for any relation $\mathcal{P}$,

$$TC(Incl^{\mathcal{P}'}(\mathcal{P})) = \mathcal{P} \Leftrightarrow TC(\mathcal{P}) = \mathcal{P} \text{ and } Incl^{\mathcal{P}'}(\mathcal{P}) = \mathcal{P}$$

If we look at semantical conditions in Definition 4 we notice that there are no closure conditions for constraints $(a), (b)$ and $(e)$. We prove that the closure conditions on $TC$, $Incl^{R_K}(\leq)$ and $1SR(R_K) = R_K$ are sufficient to characterize M-ACL semantics. We previously noticed that $(a)$ and $(b)$ are redundant with the adopted equivalent definition of $\tau_x(K \Rightarrow K')$ and $\tau_x(\Box_K \varphi)$ (see Definition 10) while, in Observation 1, we show that $(e)$ is implied by conditions $(b)$,$(c)$ and $(d)$. □

## 6 FOL Theorem Proving for M-ACL

SPASS[9] is an automated theorem prover for full first-order logic with equality [16], in this section we show how to employ SPASS to reason about M-ACL access control policies.

The use of SPASS theorem prover is based on the soundness and completeness result of M-ACL and, in particular on the identification of the canonical properties of its axioms which can be expressed as first-order constraints on Kripke structures. Moreover, in Definition 10 we showed an embedding of M-ACL formulas into FOL by relying on the definition of satisfiability. In order to use SPASS to do sound and complete deductions in M-ACL, we developed a parser called `macl2spass` which translates M-ACL formulas into first-order formulas. The translation is similar to the one in Definition 10 and it is based on standard embedding of modal logic into FOL [15].

```
list_of_formulae(axioms)
[](admin,deletefile1) -> deletefile1.
[](admin, ([](bob, deletefile1) -> deletefile1)).
[](bob, deletefile1).
end_of_list
list_of_formulae(conjectures)
deletefile1.
end_of_list
```

**Figure 1.** `example.macl`

**Example 2** *We illustrate how to use* `macl2spass` *to reason about access control policies with a (very simple) example*[10]*. Consider a file-scenario with an administrating principal* `admin`*, a user* `Bob`*, one file* `file1`*, and the following policy:*

*(1)* `admin` *says that the* `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`.

In Figure 6 we report the content of file `example.macl` which represents Example 2 using M-ACL syntax [11]. The file is divided in two parts, the policies (represented as `axioms`) and the `conjectures` which are the formulas that we want to prove from the axioms.

Once we have the M-ACL specification of the policy we can translate it into SPASS syntax with `$ ./macl2spass example.macl > exmaple.dfg`. The above command translates the M-ACL example into a first-order problem in DFG syntax[12]. The `example.dfg` can be directly given as input to SPASS theorem prover to check if the conjectures follow from the axioms.

## 7 Related Work

The formal study of properties of access control logics is a recent research trend. As reported in [11], constructive logics are well suited for reasoning about authorization, because constructive proofs preserve the justification of statements during reasoning and, therefore, information about accountability is not lost. Classical logics, instead, allows proofs that discard evidence. For example, we can prove $G$ using a classical logic by proving $F \rightarrow G$ and $\neg F \rightarrow G$, since from these theorems we can conclude $(F \vee \neg F) \rightarrow G$, hence $\top \rightarrow G$.

Abadi in [1] presents a formal study about connections between many possible axiomatizations of the says, as well as higher level policy constructs such as delegation (speaks-for) and control. Abadi provides a strong argument to use constructivism in logic for access control, in fact he shows that from a well-known axiom like Unit in a classical logic we can deduce $K$ says $\varphi \rightarrow (\varphi \vee K$ says $\psi)$. The axiom above is called *Escalation* and it represents a rather degenerate interpretation of says, i.e., if a principal says $\varphi$ then, either $\varphi$ is permitted or the principal can says *anything*. On the contrary, if we interpret the says within an intuitionistic logic we can avoid Escalation.

Even if there exist several authorization logics that employ the says modality, a limited amount of work has been done to study the formal logical properties of says, speaks-for and other constructs. In the following, we report the three different approaches adopted to study access control logics themselves.

Garg and Abadi [9] translate existing access control logics into S4 by relying on a slight simplification of Gödel's translation from intuitionistic logic to S4, and extending it to formulas of the form $A$ says $\varphi$.

Garg [8] adopts an ad-hoc version of constructive S4 called $\text{DTL}_0$ and embeds existing approaches into it. Constructive S4 has been chosen because of its intuitionistic Kripke semantics which $\text{DTL}_0$ extends by adding *views* [8], i.e., a mapping from worlds to sets of principals.

Boella et al. [5] define a logical framework called FSL[13], based on Gabbay's Fibring semantics [6] by looking at says as a (fibred) modal operator.

However, adopting a fixed semantics like S4 does not permit to study the *correspondence theory* between axioms of access control logics and Kripke structures. Suppose we look at says as a principal indexed modality $\Box_K$, if we rely on S4 we would have as an axiom $\Box_K \varphi \rightarrow \varphi$, which means: *everything* that $K$ says is permitted. To overcome this problem, both in [8, 9], Kripke semantics is sweetened

[9] SPASS is available at http://spass.mpi-sb.mpg.de
[10] More complex examples can be found in the source package of macl2spass which is available at http://www.di.unito.it/∼genovese/tools.html .
[11] `[](bob,deletefile1)` stands for $\Box_{bob} deletefile1$.
[12] http://www.spass-prover.org/webspass/help/syntax/index.html
[13] Fibred Security Language.

with the addition of *views* which relativize the reasoning to a subset of worlds. Although this approach provides sound and complete semantics, it breaks the useful bound between modality axioms and relations of Kripke structures.

The third approach, instead, shows a precise connection between axioms of access control logics and the underlying fibred semantics, but suffers from being generally undecidable and from not having an efficient methodology to reason about policies.

| Name | Problem | LEO | SPASS |
|---|---|---|---|
| unit | `s -> [](A, s)` | 0.031 | 0.02 |
| K | `[](A, s -> t) -> [](A, s) -> [](A, t)` | 0.083 | 0.02 |
| idem | `[](A, [](A, s)) -> [](A, s)` | 0.037 | 0.02 |
| refl | `A => A` | 0.052 | 0.02 |
| trans | `(A => B) -> (B => C) -> (A => C)` | 0.105 | 0.08 |
| sp.-for | `(A => B) -> [](A, s) -> [](B, s)` | 0.062 | 0.07 |
| handoff | `[](B, A => B) -> A => B` | 0.036 | 0.02 |
| Ex.1 | Example 1 | 3.494 | 0.18 |
| Ex.2 | Example 2 | 0.698 | 0.21 |

**Figure 2.** Comparison of SPASS performance against LEO-II

In [3], the higher-order theorem prover LEO-II [4] is used to reason about access control logics presented in [9] by exploiting an embedding from modal logic S4 into simple type theory. In our approach, the direct mapping of M-ACL semantics into FOL allows us to use a pure FOL theorem prover like SPASS which is generally faster than LEO-II. In Fig. 2 we compare time performance of LEO-II (taken from [3]) with SPASS[14]. We notice that in Ex.1 and Ex.2, which require more deductive steps than proving single axioms, SPASS is significantly faster then LEO-II.

## 8 Conclusions

In this paper we introduce Modal Access Control Logic, a constructive propositional multimodal logic to reason about access control policies.

We formalize a standard (i.e., without views) Kripke semantics for Modal Access Control Logic. We provide canonical properties for well known access control axioms like (Unit), (C), (handoff) and (speaking-for). We give a semantical interpretation of the speaks-for construct and we study how it relates with the says modality. We provide soundness and completeness results for M-ACL by employing a *standard* constructive semantics. We show a new application of the technique presented in [2] to prove decidability of M-ACL. We present an embedding of M-ACL into FOL and use it to reason with SPASS theorem prover.

M-ACL is the result of a new methodology in studying access control logics. In M-ACL we do not translate existing approaches into another logic (like S4 in [9]), or enrich the semantics with ad-hoc functions (like views in [8]). We show that by looking at the says operator as an universal modality we can use Kripke semantics not only to map axioms with structural properties on models, but also to use state-of-the-art theorem provers to reason about access control. By means of the translation into SPASS we show that semantics can be directly employed to reason about access control policies and that a semantics-based study of access control can benefit foundations and applications.

As future work we plan to extend M-ACL with compound principals by using semantics of conditional logics. Another line of research is to apply M-ACL to proof-carrying authorization, by developing a sequent calculus for M-ACL to exchange compact proofs about access control in a distributed environment.

[14] All the experiments with SPASS were conducted with SPASS version 3.0 on a computer with an Intel Pentium 2.53 GHz processor with 1.5GB memory running Linux.

**Acknowledgments** Valerio Genovese is supported by the National Research Fund, Luxembourg. The authors would like to thank Christoph Weidenbach, Renate Schmidt for their help with SPASS. Gian Luca Pozzato, Laura Giordano and Valentina Gliozzi for useful comments and suggestions about the completeness proof which is based on a joint work with the first author reported in [12]. Finally, the authors thank the reviewers for their comments, which proved to be helpful for improving the clarity of the paper.

## REFERENCES

[1] Martín Abadi, 'Variations in access control logic', in *9th International Conference on Deontic Logic in Computer Science (DEON)*, pp. 96–109, (2008).

[2] Natasha Alechina and Dmitry Shkatov, 'A general method for proving decidability of intuitionistic modal logics', *J. Applied Logic*, **4**(3), 219–230, (2006).

[3] Christoph Benzmüller, 'Automating access control logics in simple type theory with LEO-II', in *Emerging Challenges for Security, Privacy and Trust, 24th IFIP TC 11 International Information Security Conference, SEC*, pp. 387–398, (2009).

[4] Christoph Benzmüller, Lawrence C. Paulson, Frank Theiss, and Arnaud Fietzke, 'LEO-II - a cooperative automatic theorem prover for classical higher-order logic (system description)', in *Automated Reasoning, 4th International Joint Conference, IJCAR*, pp. 162–170, (2008).

[5] Guido Boella, Dov M. Gabbay, Valerio Genovese, and Leendert van der Torre, 'Fibred security language', *Studia Logica*, **92**(3), 395–436, (2009).

[6] Dov M. Gabbay, 'Fibring logics', *Oxford University Press*, (1999).

[7] Harald Ganzinger, Christoph Meyer, and Margus Veanes, 'The two-variable guarded fragment with transitive relations', in *14th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pp. 24–34, (1999).

[8] Deepak Garg, 'Principal centric reasoning in constructive authorization logic', in *Informal Proceedings of Intuitionistic Modal Logic and Application (IMLA)*, (2008). Full version available as Carnegie Mellon Technical Report CMU-CS-09-120.

[9] Deepak Garg and Martín Abadi, 'A modal deconstruction of access control logics', in *11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)*, pp. 216–230, Budapest, Hungary, (2008).

[10] Deepak Garg, Lujo Bauer, Kevin D. Bowers, Frank Pfenning, and Michael K. Reiter, 'A linear logic of authorization and knowledge', in *European Symposium on Research in Computer Security (ESORICS)*, pp. 297–312, (2006).

[11] Deepak Garg and Frank Pfenning, 'Non-interference in constructive authorization logic', in *19th IEEE Computer Security Foundations Workshop, (CSFW-19), 5-7 July 2006, Venice, Italy*, pp. 283–296, (2006).

[12] V. Genovese, L. Giordano, V. Gliozzi, and G. L. Pozzato, 'A constructive conditional logic for access control: a completeness result.', in *Technical Report 125/2010, Dipartimento di Informatica, Università degli Studi di Torino, Italy*, (2010).

[13] Yuri Gurevich and Arnab Roy, 'Operational semantics for DKAL: Application and analysis', in *Trust, Privacy and Security in Digital Business, 6th International Conference (TrustBus)*, pp. 149–158, (2009).

[14] Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum, 'Delegation logic: A logic-based approach to distributed authorization', *ACM Trans. Inf. Syst. Secur.*, **6**(1), 128–171, (2003).

[15] Hans Jürgen Ohlbach, 'Semantics-based translation methods for modal logics', *J. Log. Comput.*, **1**(5), 691–746, (1991).

[16] Christoph Weidenbach, Dilyana Dimova, Arnaud Fietzke, Rohit Kumar, Martin Suda, and Patrick Wischnewski, 'SPASS version 3.5', in *Automated Deduction, 22nd International Conference on Automated Deduction (CADE)*, pp. 140–145, (2009).

[17] F. Wolter and M. Zakharyaschev, 'Intuitionistic modal logic', in *A. Cantini, E. Casari, and P. Minari, editors, Logic and Foundations of Mathematics. Kluwer Academic Publishers*, pp. 227–238, (1999).