Belief Semantics of Authorization Logic

Anonymized for submission to CCS 2013

ABSTRACT

Authorization logics have been used in the theory of computer security to reason about access control decisions. In this work, a formal belief semantics for authorization logics is given. The belief semantics is proved to subsume a Kripke semantics. The belief semantics yields a direct representation of principals' beliefs, without resorting to the technical machinery used in Kripke semantics. A proof system is given for the logic; that system is proved sound with respect to the belief and Kripke semantics. The soundness proofs for both semantics are mechanized in Coq.

Keywords

security policies, access control, logic, authorization

1. INTRODUCTION

Authorization logics are used in computer security to reason about whether *principals*—computer or human agents—are permitted to take actions in computer systems. The distinguishing feature of authorization logics is their use of a says connective: intuitively, if principal p believes that formula ϕ holds, then formula p says ϕ holds. Access control decisions can then be made by reasoning about (i) the beliefs of principals, (ii) how those beliefs can be combined to derive logical consequences, and (iii) whether those consequences entail *guard formulas*, which must hold for actions to be permitted.

Many systems that employ authorization logics have been proposed [5–9, 11, 12, 17, 23, 28, 29, 32–35, 40, 44, 51], but few authorization logics have been given a formal semantics [4, 18, 19, 22, 26]. Though semantics might not be immediately necessary to deploy authorization logics in real systems, semantics yield insight into the meaning of formulas, and semantics enable proof systems to be proved sound—which might require proof rules and axioms to be corrected, if there are any lurking errors in the proof system.

For the sake of security, it is worthwhile to carry out such soundness proofs. Given only a proof system, we must trust that the proof system is correct. But given a proof system and a soundness proof, which shows that any provable formula is semantically valid, we now have evidence that the proof system is correct, hence trustworthy. The soundness proof thus relocates trust from the proof system to the proof itself—as well as to the semantics, which ideally offers more intuition about formulas than the proof system itself.

Semantics of authorization logics are usually based on *possible worlds*, as used by Kripke [31]. *Kripke semantics* posit an indexed *accessibility relation* on possible worlds. If at world w, principal p considers world w' to be possible, then (w, w') is in p's accessibility relation. We denote this as $w \leq_p w'$. Authorization logics use Kripke semantics to give meaning to the says connective: semantically, p says ϕ holds in a world w iff for all worlds w' such that $w \leq_p w'$, formula ϕ holds in world w'. Hence a principal says ϕ iff ϕ holds in all worlds the principal considers possible.[1]

The use of Kripke semantics in authorization logic thus requires installation of possible worlds and accessibility relations into the semantics, solely to give meaning to says. That's useful for studying properties of logics and for building decision procedures. But, unfortunately, it doesn't seem to correspond to how principals reason in real-world systems. Rather than explicitly considering possible worlds and relations between them, principals typically begin with some set of base formulas they believe to hold—perhaps because they have received digitally signed messages encoding those formulas, or perhaps because they invoke system calls that return information—then proceed to reason from those formulas. So could we instead stipulate that each principal p have a set of beliefs $\omega(p)$, called the *worldview* of p, such that p says ϕ holds iff $\phi \in \omega(p)$? That is, a principal says ϕ iff ϕ is in the worldview[2]of the principal?

This paper answers that question in the affirmative. We give two semantics for an authorization logic: a Kripke semantics (§3), and a new *belief semantics* (§2), which employs worldviews to interpret says.[3] We show (§4) that belief semantics subsume Kripke semantics, in the sense that a belief model can be constructed from any Kripke model. A formula is valid in the Kripke model iff it is valid in the constructed belief model. As a result, the technical machinery of Kripke

CCS'13 Berlin, Germany

[1]The says connective is, therefore, closely related to the modal necessity operator $\Box$ [27] and the epistemic knowledge operator K [15].

[2]Worldviews were first employed by NAL [42], which pioneered an informal semantics based on them.

[3]Our belief models are an instance of the *syntactic* approach to modeling knowledge [13, 15, 30, 37].

semantics can be replaced by belief semantics. This potentially increases the trustworthiness of an authorization system, because the semantics is closer to how principals reason in real systems.

The particular logical system we introduce in this paper is FOCAL, First-Order Constructive Authorization Logic. FOCAL extends a well-known authorization logic, cut-down dependency core calculus (CDD) [2], from a propositional language to a language with first-order functions and relations on system state. Functions and relations are essential for reasoning about authorization in a real operating system—as exemplified in Nexus Authorization Logic (NAL) [42], of which FOCAL is a fragment.

Having given two semantics for FOCAL, we then turn to the problem of proving soundness. It turns out that the NAL proof system is unsound with respect to the semantics presented here: NAL allows derivation of a well-known formula (cf. §5.2) that our semantics deems invalid. A priori, the fault could lie with our semantics or with NAL's proof system. However, if the logic is to be used in a distributed setting without globally-agreed upon state, then the proof system should not allow the formula to be derived. So if NAL is to be used in such settings, its proof system needs to be corrected.

NAL extends CDD, so CDD is also unsound with respect to our semantics. However, CDD has been proved sound with respect to a different semantics [19]. This seeming discrepancy—sound vs. unsound—illuminates a previously unexplored difference (cf. §5.2) between how NAL and CDD interpret says.

To achieve soundness for FOCAL, we develop a revised proof system; the key technical change is using localized hypotheses in the proof rules. In §5, we prove the soundness of our proof system with respect to both our belief and Kripke semantics. This result yields the first soundness proof with respect to belief semantics for an authorization logic.

Having relocated trust into the soundness proof, we then seek a means to increase the trustworthiness of that proof. We formalize the syntax, proof system, belief semantics, and Kripke semantics in the Coq proof assistant,[4] and we mechanize the proofs of soundness for both the belief semantics and the Kripke semantics. That mechanization relocates trust from our soundness proof to Coq, which is well-studied and is the basis of many other formalizations. Our Coq formalization contains about 2,400 lines of code.[5]

This paper thus advances the theory of computer security with the following novel contributions:

- the first formal belief semantics for authorization logic,
- a proof of equivalence between belief semantics and Kripke semantics,
- a proof system that is sound with respect to belief and Kripke semantics, and
- the first machine-checked proof of soundness for an authorization-logic proof system.

We proceed as follows. §2 presents FOCAL and its belief semantics. §3 gives a Kripke semantics for FOCAL. §4 proves the relationship of the belief semantics to the Kripke semantics. §5 gives a proof system for FOCAL and proves its soundness with respect to the Kripke semantics. §6 discusses related work, and §7 concludes. All proofs appear in appendix A.

[4] `http://coq.inria.fr`

[5] Our anonymized implementation is available from `https://github.com/focal-research/focal`.

$$
\begin{array}{rcl}
\tau & ::= & x \mid f(\tau, \ldots, \tau) \\
\phi & ::= & \mathsf{true} \mid \mathsf{false} \mid r(\tau, \ldots, \tau) \mid \tau_1 = \tau_2 \\
& \mid & \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \Rightarrow \phi_2 \mid \neg\phi \\
& \mid & (\forall\, x : \phi) \mid (\exists\, x : \phi) \\
& \mid & \tau \ \mathsf{says}\ \phi \mid \tau_1 \ \mathsf{speaksfor}\ \tau_2
\end{array}
$$

Figure 1: Syntax of FOCAL

2. BELIEF SEMANTICS

FOCAL is a constructive, first-order, multimodal logic. The key features that distinguish it as an authorization logic are the says and speaksfor connectives, invented by Lampson et al. [32]. These are used to reason about authorization—for example, access control in a distributed system can be modeled in the following standard way:

Example 1. *A* guard *implements access control for a printer p. To permit printing to p, the guard must be convinced that guard formula PrintServer* says *printTo(p) holds, where PrintServer is the principal representing the server process. That formula means that PrintServer believes printTo(p) holds. To grant printer access to user u, the print server can issue the statement u* speaksfor *PrintServer. That formula means anything u says, the PrintServer must also say. So if u* says *printTo(p), then PrintServer* says *printTo(p), which satisfies the guard formula hence affords the user access to the printer.*

Figure 1 gives the formal syntax of FOCAL. There are two syntactic classes, terms τ and formulas ϕ. Metavariable x ranges over first-order variables, f over first-order functions, and r over first-order relations.

Formulas of FOCAL do not permit monadic second-order universal quantification, unlike CDD and NAL. In NAL, which is an extension of CDD, that quantifier was used only to define false and speaksfor as syntactic sugar. FOCAL instead adds these as primitive connectives to the logic. Negation $\neg\phi$ could be defined as syntactic sugar for $\phi \Rightarrow \mathsf{false}$.

2.1 Semantic models

The belief semantics of FOCAL combines first-order constructive models with worldviews, which are used to interpret says and speaksfor. To our knowledge, this semantics is new in the study of authorization logics. Our presentation mostly follows the semantics of intuitionistic predicate calculus given by Troelstra and van Dalen [47].

First-order models. A *first-order model with equality* is a tuple $(D, =, R, F)$. The purpose of a first-order model is to interpret the first-order fragment of the logic, specifically first-order quantification, functions, and relations. D is a set, the *domain* of individuals. Semantically, quantification in the logic ranges over these individuals. R is a set $\{r_i \mid i \in I\}$ of relations on D, indexed by set I. Likewise,

F is a set $\{f_j \mid j \in J\}$ of functions on D, indexed by set J. There is a distinguished equality relation $=$, which is an equivalence relation on D, such that equal individuals are indistinguishable by relations and functions.

To interpret first-order variables, the semantics employs *valuation* functions, which map variables to individuals. We write $v(x)$ to denote the individual that variable x represents in valuation v.

Constructive models. A *constructive model* is a tuple $(W, \leq, s)$. The purpose of constructive models is to extend first-order models to interpret the constructive fragment of the logic, specifically implication and universal quantification. W is a set, the possible worlds. We denote an individual world as w. Intuitively, a world w represents the state of knowledge of a constructive reasoner. *Constructive accessibility relation* $\leq$ is a partial order on W. If $w \leq w'$, then the constructive reasoner's state of knowledge could grow from w to w'. Function s is the *first-order interpretation function*. It assigns a first-order model $(D_w, =_w, R_w, F_w)$ to each world w. Let the individual elements of R_w be denoted as $r_{i,w}$, and the elements of F_w as $f_{j,w}$. Thus, s enables a potentially different first-order interpretation at each world. But to help ensure that the constructive reasoner's state of knowledge only grows—hence never invalidates a previously admitted construction—we require s to be monotonic w.r.t. $\leq$. That is, if $w \leq w'$ then (i) $D_w \subseteq D_{w'}$, (ii) $d =_w d'$ implies $d =_{w'} d'$, (iii) $r_{i,w} \subseteq r_{i,w'}$, and (iv) for all tuples $\vec{d}$ of individuals, it holds that $f_{j,w}(\vec{d}) =_w f_{j,w'}(\vec{d})$.

It's natural to wonder why we chose to introduce possible worlds into the semantics here after arguing against them in §1. Note, though, that the worlds in the constructive model are being used to model only the constructive reasoner—which we might think of as the guard, who exists outside the logic and attempts to ascertain the truth of formulas—not any of the principals reasoned about inside the logic. Moreover, we have not introduced any accessibility relations for principals, but only a single accessibility relation for the constructive reasoner. So the arguments in §1 don't apply. It would be possible to eliminate our usage of possible worlds by employing a *Heyting algebra semantics* [48] of constructive logic. But possible worlds blend better with the Kripke semantics in §3.

It's also natural to wonder why FOCAL is constructive rather than classical. Schneider et al. [42] write that constructivism preserves evidence: "Constructive logics are well suited for reasoning about authorization... because constructive proofs include all of the evidence used for reaching a conclusion and, therefore, information about accountability is not lost. Classical logics allow proofs that omit evidence." Garg and Pfenning [20] also champion the notion of evidence in authorization logics, writing that "[constructive logics] keep evidence contained in proofs as direct as possible." So we chose to make FOCAL constructive for the sake of evidence. Regardless, we believe that a classical version of FOCAL could be created without difficulty.

Belief models. A *belief model* is a tuple $(W, \leq, s, P, \omega)$. The purpose of belief models is to extend constructive models to interpret says and speaksfor. The first part of a belief model, $(W, \leq, s)$, must itself be a constructive model. The next part, P, is the set of principals. Although individuals can vary from world to world in a model, the set of principals is fixed across the entire model. Assuming a fixed set of principals is consistent with other authorization logics [18, 19, 22], with constructive multimodal logics [43, 50] (which have a fixed set of modalities), and with classical multimodal epistemic logics [15] (which have an indexed set modalities, typically denoted K_i, where the index set is fixed)—even though constructivist philosophy might deem it more sensible to allow P to grow with $\leq$.

Because we make no syntactic distinction between individuals and principals, all principals must also be individuals: P must be a subset of D_w for every w. First-order quantification can therefore range over individuals as well as principals. For example, to quantify over all principals, we can write $(\forall x : \mathit{IsPrin}(x) \Rightarrow \phi)$, where *IsPrin* is a relation that holds for all $x \in P$. We define an equality relation $\doteq$ on principals, such that principals are equal iff they are equal at all worlds. Formally, $p \doteq p'$ iff, for all w, it holds that $p =_w p'$.

The final part of a belief model, worldview function ω, yields the beliefs of a principal p: the set of formulas that p believes to hold in world w under first-order valuation v is $\omega(w, p, v)$. For sake of simplicity, §1 used notation $\omega(p)$ when first presenting the idea of worldviews. Now that we're being precise, ω needs w as an argument. We also add v as an additional argument, because it makes the equivalence result of §4 provable. To ensure that the constructive reasoner's knowledge grows monotonically, worldviews must be monotonic w.r.t. $\leq$:

> **Worldview Monotonicity:** If $w \leq w'$ then $\omega(w, p, v) \subseteq \omega(w', p, v)$.

And to ensure that whenever principals are equal they have the same worldview, we require the following:

> **Worldview Equality:** If $p \doteq p'$, then, for all w and v, it holds that $\omega(w, p, v) = \omega(w, p', v)$.

2.2 Semantic validity

Figure 2 gives a belief semantics of FOCAL. The validity judgment is written $B, w, v \models \phi$ where B is a belief model and w is a world in that model. As is standard, $B \models \phi$ holds iff, for all w and v, it holds that $B, w, v \models \phi$; whenever $B \models \phi$, then ϕ is a *necessary* formula in model B. And $B, v \models \phi$ holds iff for all w, it holds that $B, w, v \models \phi$; whenever $B, v \models \phi$, then ϕ is a *valuation-necessary* formula. Likewise, $\models \phi$ holds iff, for all B, it holds that $B \models \phi$; and whenever $\models \phi$, then ϕ is a *validity*. Let $B, w, v \models \Gamma$, where Γ is a set of formulas, denote that for all $\psi \in \Gamma$, it holds that $B, w, v \models \psi$. Let $B \models \Gamma$ denote that, for all w and v, it holds that $B, w, v \models \Gamma$. Finally, $\Gamma \models \phi$ holds iff, for all B, it holds that $B \models \Gamma$ implies $B \models \phi$; whenever $\Gamma \models \phi$, then ϕ is a *logical consequence* of Γ.

The semantics relies on an auxiliary *interpretation* function μ that maps syntactic terms τ to semantic individuals:

$$\mu(x) = v(x)$$
$$\mu(f_j(\vec{\tau})) = f_{j,w}(\mu(\vec{\tau}))$$

Implicitly, μ is parameterized on belief model B, world w, and valuation v, but for notational simplicity we omit writing these as arguments to μ unless necessary for disambiguation. Variables x are interpreted by looking up their value in v; functions f_j are interpreted by applying their first-order interpretation $f_{j,w}$ at world w to the interpretation of

$$
\begin{array}{lll}
B, w, v \models \mathsf{true} & & \text{always} \\
B, w, v \models \mathsf{false} & & \text{never} \\
B, w, v \models r_i(\vec{\tau}) & \text{iff} & \mu(\vec{\tau}) \in r_{i,w} \\
B, w, v \models \tau_1 = \tau_2 & \text{iff} & \mu(\tau_1) =_w \mu(\tau_2) \\
B, w, v \models \phi_1 \wedge \phi_2 & \text{iff} & B, w, v \models \phi_1 \text{ and } B, w, v \models \phi_2 \\
B, w, v \models \phi_1 \vee \phi_2 & \text{iff} & B, w, v \models \phi_1 \text{ or } B, w, v \models \phi_2 \\
B, w, v \models \phi_1 \Rightarrow \phi_2 & \text{iff} & \text{for all } w' \geq w : B, w', v \models \phi_1 \text{ implies } B, w', v \models \phi_2 \\
B, w, v \models \neg\phi & \text{iff} & \text{for all } w' \geq w : B, w', v \not\models \phi \\
B, w, v \models (\forall\, x : \phi) & \text{iff} & \text{for all } w' \geq w, d \in D_{w'} : B, w', v[d/x] \models \phi \\
B, w, v \models (\exists\, x : \phi) & \text{iff} & \text{there exists } d \in D_w : B, w, v[d/x] \models \phi \\
B, w, v \models \tau \ \mathsf{says}\ \phi & \text{iff} & \phi \in \omega(w, \mu(\tau), v) \\
B, w, v \models \tau_1 \ \mathsf{speaksfor}\ \tau_2 & \text{iff} & \text{for all } w' \geq w : \omega(w', \mu(\tau_1), v) \subseteq \omega(w', \mu(\tau_2), v)
\end{array}
$$

Figure 2: FOCAL validity judgment for belief semantics

their arguments. Notation $\vec{\tau}$ represents a list $\tau_1, \tau_2, \ldots, \tau_n$ of terms. And $\mu(\vec{\tau})$ denotes the pointwise application of μ to each element of that list, producing $\mu(\tau_1), \ldots, \mu(\tau_n)$.

The first-order, constructive fragment of the semantics is routine. The semantics of says is the intuitive semantics we wished for in §1: A principal $\mu(\tau)$ says ϕ exactly when ϕ is in that principal's worldview $\omega(w, \mu(\tau), v)$. And a principal $\mu(\tau_1)$ speaks for another principal $\mu(\tau_2)$ exactly when, in all constructively accessible worlds, everything $\mu(\tau_1)$ says, $\mu(\tau_2)$ also says.

Note that some syntactic terms may represent individuals that are not principals. For example, the integer 42 is presumably not a principal in P, but it could be an individual in some domain D_w. An alternative would be to make FOCAL a two-sorted logic, with one sort for individuals and another sort for principals. Instead, we allow individuals who aren't principals to have beliefs, because it simplifies the definition of the logic. The worldviews of non-principal individuals contain only those formulas that all principals' worldviews would also be forced to contain. Formally, for any individual d such that $d \notin P$, and for any world w and valuation v, worldview $\omega(w, d, v)$ is set $\{\phi \mid B, v \models \phi\}$ of all valuation-necessities.

We impose a few *well-formedness* conditions on worldviews in this semantics, in addition to Worldview Monotonicity and Worldview Equality. Worldviews must be *closed under logical consequence*—that is, principals must believe all the formulas that are a consequence of their beliefs.

> **Worldview Closure:** If $\Gamma \subseteq \omega(w, p, v)$ and $\Gamma \models \phi$, then $\phi \in \omega(w, p, v)$.

Worldview Closure means that principals are *fully logically omniscient* [15]. With its known benefits and flaws [39, 46], this has been a standard assumption in authorization logics since their inception [32].

The remaining well-formedness conditions are optional, in the sense that they are necessary only to achieve soundness of particular proof rules in §5. Eliminate those rules, and the following conditions would be eliminated.

Worldviews must ensure that says is a *transparent* modality. That is, for any principal p, it holds that p says ϕ exactly when p says (p says ϕ):

> **Says Transparency:** $\phi \in \omega(w, \mu(\tau), v)$ iff τ says $\phi \in \omega(w, \mu(\tau), v)$.

So says supports *positive introspection*: if p believes that ϕ holds, then p is aware of that belief, therefore p believes that p believes that ϕ holds. The converse of that holds as well. Recent authorization logics include transparency [3, 42], and it is well known (though sometimes vigorously debated) in epistemic logic [25, 27]. Says Transparency corresponds to rules SAYS-LI and SAYS-RI in figure 5.

Worldviews must enable principals to delegate, or *hand-off*, to other principals: if a principal q believes that p speaksfor q, it should hold that p does speak for q. Hand-off, as the following axiom, existed in the earliest authorization logic [32]:

$$(q \ \mathsf{says}\ (p \ \mathsf{speaksfor}\ q)) \Rightarrow (p \ \mathsf{speaksfor}\ q) \tag{1}$$

To support it, we adopt a condition that ensures whenever q believes p speaks for q, then it really does:

> **Belief Hand-off:** If (p speaksfor q) $\in \omega(w, q, v)$ then $\omega(w, p, v) \subseteq \omega(w, q, v)$.

Belief Hand-off corresponds to rule SF-I in figure 5.

3. KRIPKE SEMANTICS

The Kripke semantics of FOCAL combines first-order constructive models with modal (Kripke) models [15, 27, 43]. Similar semantic models have been explored before (see, e.g., [18, 22, 50]). Indeed, the only non-standard part of our semantics is the treatment of speaksfor, and that part turns out to be a generalization of previous classical semantics. Nonetheless, we are not aware of any authorization logic semantics that is equivalent to or subsumes our semantics. First-order and constructive models were already presented in §2, so we begin here with modal models.

3.1 Modal models

A *modal model* is a tuple $(W, \leq, s, P, A)$. The purpose of modal models is to extend constructive models to interpret says and speaksfor. The first part of a modal model, $(W, \leq, s)$, must itself be a constructive model. The next part, P, is the set of principals. As with belief models, all principals must be individuals, so P must be a subset of D_w for every w. Principal equality relation $\doteq$ is defined just as in belief models. The final part of a modal model, A, is a set $\{\leq_p \mid p \in P\}$ of binary relations on W, called the *principal accessibility relations*.[6] If $w \leq_p w'$, then at world

[6] In our notation, an unsubscripted $\leq$ always denotes the constructive relation, and a subscripted $\leq$ always denotes a principal relation.

$$
\begin{array}{lll}
K, w, v \models \tau \text{ says } \phi & \text{iff} & \text{for all } w', w'' : w \leq w' \leq_{\mu(w',\tau)} w'' \text{ implies } K, w'', v \models \phi \\
K, w, v \models \tau_1 \text{ speaksfor } \tau_2 & \text{iff} & \leq^w_{\mu(\tau_1)} \supseteq \leq^w_{\mu(\tau_2)} \\
K, w, v \models \ldots & \text{iff} & \textit{same as figure 2, but substituting } K \textit{ for } B
\end{array}
$$

Figure 3: FOCAL validity judgment for Kripke semantics

w, principal p considers world w' possible. To ensure that equal principals have the same beliefs, we require

Accessibility Equality: If $p \doteq p'$, then $\leq_p = \leq_{p'}$.

Like $\leq$ in a constructive model, we require s to be monotonic w.r.t. each $\leq_p$. This requirement enforces a kind of constructivity on each principal p, such that from a world in which individual d is constructed, p cannot consider possible any world in which d has not been constructed. Unlike $\leq$, none of the $\leq_p$ are required to be partial orders: they are not required to satisfy reflexivity, anti-symmetry, or transitivity.

That non-requirement raises an important question. In epistemic logics, the properties of what we call the "principal accessibility relations" determine what kind of knowledge is modeled [15]. If, for example, these relations must be reflexive, then the logic models *veridical* knowledge: if p says ϕ, then ϕ indeed holds. But that is not the kind of knowledge we seek to model with FOCAL, because principals may say things that in fact do not hold. So what are the right properties, or *frame conditions*, to require of our principal accessibility relations? We briefly delay presenting them, so that we can present the Kripke semantics.

3.2 Semantic validity

Figure 3 gives a Kripke semantics of FOCAL. The validity judgment is written $K, w, v \models \phi$ where K is a modal model and w is a world in that model. Only the judgments for the says and speaksfor connectives are given in figure 3. For the remaining connectives, the Kripke semantics is the same as the belief semantics in figure 2. Interpretation function μ remains unchanged from §2, except that it is now implicitly parameterized on K instead of B.

To understand the semantics of says, first observe the following. Suppose that, for all worlds w', it holds that $w \leq w'$ implies $w = w'$.[7] Then the semantics of says simplifies to the standard semantics of $\Box$ in classical modal logic [27]:

$$
\begin{array}{l}
K, w, v \models \tau \text{ says } \phi \\
\qquad \text{iff} \quad \text{for all } w'' : w \leq_{\mu(\tau)} w'' \text{ implies } K, w, v \models \phi.
\end{array}
$$

That is, a principal believes a formula holds whenever that formula holds in all accessible worlds. The purpose of the quantification over w', where $w \leq w'$, in the unsimplified semantics of says is to achieve *monotonicity* of the constructive reasoner:

PROPOSITION 1. *If* $K, w, v \models \phi$ *and* $w \leq w'$ *then* $K, w', v \models \phi$.

That is, whenever ϕ holds at a world w, if the constructive reasoner is able to reach an extended state of knowledge at world w', then ϕ should continue to hold at w'. Without the quantification over w' in the semantics of says, monotonicity is not guaranteed to hold. Constructive modal logics have, unsurprisingly, also used this semantics for $\Box$ [43, 50], and a similar semantics has been used in authorization logic [18].

Note that, if there do not exist any worlds w' and w'' such that $w \leq w' \leq_{\mu(\tau)} w''$, then at w, principal τ will say any formula ϕ, including false. When a principal says false at world w, we deem that principal *compromised* at w.

As for the semantics of speaksfor, it might be tempting to try defining it as syntactic sugar:

$$\tau_1 \text{ speaksfor } \tau_2 \quad \equiv \quad \forall \phi : \tau_1 \text{ says } \phi \Rightarrow \tau_2 \text{ says } \phi$$

However, the formula on the right-hand side is not a well-formed formula of FOCAL, because it quantifies over syntactic formulas. So the semantics of speaksfor cannot interpret it directly in terms of says.[8]

Instead, the FOCAL semantics of speaksfor generalizes the classical Kripke semantics of speaksfor [4, 26]. Classically,

$$K, w, v \models \tau_1 \text{ speaksfor } \tau_2 \quad \text{iff} \quad \leq_{\mu(\tau_1)} \supseteq \leq_{\mu(\tau_2)}. \qquad (2)$$

That is, the accessibility relation of τ_1 must be a superset of the accessibility relation of τ_2. However, that definition does not account for constructive accessibility, and it even turns out to interact badly with hand-off (cf. §3.4).

We therefore relax the classical semantics of speaksfor:

$$K, w, v \models \tau_1 \text{ speaksfor } \tau_2 \quad \text{iff} \quad \leq^w_{\mu(\tau_1)} \supseteq \leq^w_{\mu(\tau_2)} \qquad (3)$$

where $\leq^w_{\mu(p)}$ is defined to be $\leq_p |_{[w]_p}$,[9] and $[w]_p$ is defined to be the set of worlds w' such that w' is reachable from w, or vice-versa, by relation $(\leq \cup \leq_p)^*$. Note that whenever $[w]_p$ equals W (as it would in classical logic[10]), it holds that $\leq^w_{\mu(p)}$ equals $\leq_p$.

The validity judgment for FOCAL is therefore quite standard, except for speaksfor, where it generalizes classical logic. Although we would prefer to adopt a well-known constructive semantics of speaksfor, neither of the two we're aware of seems to work for FOCAL: ICL [19] would impose an axiom called Unit that we do not want to include (cf. §5.2), and BL_{sf} [22] does not include hand-off (1), which we do want.

3.3 Frame conditions

We now return to the discussion begun in §3.1 of the frame conditions for FOCAL. The first two frame conditions we impose help to ensure Says Transparency:

[7] This condition corresponds to the axiom of excluded middle, hence its imposition creates a classical variant of FOCAL. So it makes sense that adding the frame condition would result in the classical semantics of $\Box$.

[8] It is possible [19, 42] to instead use second-order quantifiers to achieve a direct interpretation. That solution would unnecessarily complicate our semantics by introducing second-order quantifiers solely for the sake of defining speaksfor.

[9] If R is a binary relation on set A, then $R|_X$ is the *restriction* of R to A, where $X \subseteq A$. That is, $R|_X = \{(x, x') \mid (x, x') \in R \text{ and } x \in X \text{ and } x' \in X\}$.

[10] When frame condition $\leq = W \times W$ is imposed, constructive logic collapses to classical. Under that condition, every world w' would be reachable from w, hence $[w]_p = W$.

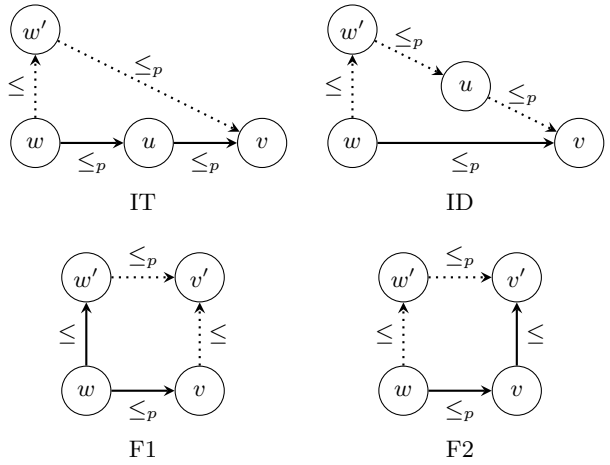

Figure 4: Frame conditions for Kripke semantics

> **IT:** If $w \leq_p u \leq_p v$, then there exists a w' such that $w \leq w' \leq_p v$.
>
> **ID:** If $w \leq_p v$, then there exists a w' and u such that $w \leq w' \leq_p u \leq_p v$.

Figure 4 depicts these conditions; dotted lines indicate existentially quantified edges. IT helps to guarantee if p says ϕ then p says (p says ϕ); ID does the converse.[11]

Note how, if $w = w'$, the conditions reduce to the classical definitions of transitivity and density. Those classical conditions are exactly what guarantee transparency in classical modal logic.

IT and ID are not quite sufficient to yield transparency. By also imposing the following frame condition, we do achieve transparency:[12]

> **F2:** If $w \leq_p v \leq v'$, then there exists a w' such that $w \leq w' \leq_p v'$.

F2 is depicted in figure 4. It is difficult to motivate F2 solely in terms of authorization logic, though it has been proposed in several Kripke semantics for constructive modal logics [14, 16, 41, 43]. But there are two reasons why F2 is desirable for FOCAL:

- Assuming F2 holds, IT and ID are not only sufficient but also necessary conditions for transparency—a result that follows from work by Plotkin and Stirling [41]. So in the presence of F2, transparency in FOCAL is precisely characterized by IT and ID.

- Suppose FOCAL were to be extended with a $\Diamond$ modality. It could be written τ suspects ϕ, with semantics $K, w, v \models \tau$ suspects ϕ iff there exists w' such that $w \leq_{\mu(\tau)} w'$ and $K, w', v \models \phi$. We would want says and suspects to interact smoothly. For example, it would be reasonable to expect that $\neg(\tau$ suspects $\phi)$ implies τ says $\neg\phi$. For if τ does not suspect ϕ holds anywhere, then τ should believe $\neg\phi$ holds. Condition F2 guarantees that implication [41]. So F2 prepares FOCAL for future extension with a suspects modality.[13]

To ensure the validity of hand-off, we impose the following frame condition:

> **H:** For all principals p and worlds w, if there do not exist any worlds w' and w'' such that $w \leq w' \leq_p w''$, then, for all p', it must hold that $\leq^w_{\mu(p)} \subseteq \leq^w_{\mu(p')}$.

This condition guarantees that if a principal p becomes compromised at world w, then the reachable component of its accessibility relation will be a subset of all other principals'. By the FOCAL semantics of speaksfor, all other principals therefore speak for p at w.

Each frame condition above was imposed, not for ad hoc purposes, but because of a specific need in the proof of the soundness result of §5. So with appropriate deletion of rules from the proof system, each of the above frame conditions could be eliminated. IT and ID should be removed if rules SAYS-LI and SAYS-RI (from figure 5) are removed; F2 should be removed if rule SAYS-LRI is removed; and H should be removed if rule SF-I is removed.

Finally, we impose one additional condition to achieve the equivalence result of §4:

> **WSF:** $K, w, v \models \tau$ speaksfor τ' iff, for all ϕ, if $K, w, v \models \tau$ says ϕ, then $K, w, v \models \tau'$ says ϕ.

This condition restricts the class of Kripke models to those where speaksfor is the *weak speaksfor* connective [4, 26]. In fact, we'd prefer to use WSF directly as the semantics of speaksfor. But it isn't a well-founded definition of $\models$, because ϕ could itself be τ speaksfor τ', leading to a circularity in the semantic definition. Coq's type theory, in fact, prohibits this definition for that very reason.

3.4 Defining Speaksfor

Abadi [3] presents several strange consequences of classical authorization logic. Here is yet another that results when we try to use the classical definition of speaksfor (2) in a constructive setting:

EXAMPLE 2. *Consider a world w. Suppose there do not exist any worlds w' and w'' such that $w \leq w' \leq_{\mu(\tau)} w''$. Then at world w, principal τ is compromised: it says* false*, and also says any other formula ϕ.*

Let ϕ be τ' speaksfor τ. Then it holds, for any principal τ', that $K, w, v \models \tau$ says (τ' speaksfor τ). By hand-off, we then have $K, w, v \models \tau'$ speaksfor τ. By the classical semantics of speaksfor*, we have $\leq_{\mu(\tau')} \supseteq \leq_{\mu(\tau)}$. So τ's accessibility relation must be a subset of all other principal's accessibility relations. In the extreme case, if there is a principal whose accessibility relation is empty, τ's relation must also be empty.*

Therefore, if there ever is any world w at which principal τ is compromised, then τ's accessibility relation must be

[11] IT and ID are abbreviations for intuitionistic transitivity and intuitionistic density.

[12] F2 is the name given this condition by Simpson [43].

[13] Were suspects to be added to FOCAL, it would also be desirable to impose a fourth frame condition: if $w \leq w'$ and $w \leq_p v$, then there exists a v' such that $v \leq v'$ and $w' \leq_p v'$. This condition, named F1 by Simpson [43], guarantees [41] that τ suspects ϕ implies $\neg(\tau$ says $\neg\phi)$. It also guarantees monotonicity (cf. proposition 1) for suspects. Figure 4 depicts F1. Simpson [43, p. 51] argues that F1 and F2 could be seen as fundamental, not artificial, frame conditions for constructive modal logics.

empty. That means if τ is compromised at one world, τ must be compromised at all worlds.

As a result, the constructive reasoner is immediately forced to recognize that a principal is compromised, even if the reasoner is in a minimal state of knowledge (i.e., at a world w at which there do not exist any worlds v such that $v \leq w$.) The reasoner is not allowed to wait until some greater state of knowledge to discover that a principal is compromised. This seems to be an intuitionistically undesirable feature.

But with FOCAL's definition of speaksfor (3), only the components of the accessibility relations that are locally reachable from w need to be considered. So a principal could be entirely compromised in some set of worlds not reachable from w, but that principal need not be compromised at w.

4. SEMANTIC TRANSFORMATION

We have now given two semantics for FOCAL, a belief semantics (§2) and a Kripke semantics (§3). How are these two semantics related? It turns out that a Kripke model can be transformed into a belief model, but the converse does not hold—as we now explain.

Given a modal model K, there is a natural way to construct a belief model from it: assign each principal a worldview containing exactly the formulas that the principal says in K. Call this construction *k2b*, and let $k2b(K)$ denote the resulting belief model.

To give a precise definition of *k2b*, we need to introduce a new notation. Given a principal $p \in P$, formula p says ϕ is not necessarily well-formed, because p is not necessarily a syntactic term. So let $K, w, v \models \hat{p}$ says ϕ be defined as follows: for all w' and w'' such that $w \leq w' \leq_p w''$, it holds that $K, w'', v \models \phi$. This definition simply unrolls the semantics of says to produce something well-formed.[14]

The precise definition of *k2b* is as follows: if $K = (W, \leq, s, P, A)$, then $k2b(K)$ is belief model $(W, \leq, s, P, \omega)$, where $\omega(w, p, v)$ is defined to be $\{\phi \mid K, w, v \models \hat{p}$ says $\phi\}$.

Our first concern is whether $k2b(K)$ produces a belief model that is equivalent to K. In particular, a formula should be valid in K iff it is valid in $k2b(K)$. Construction *k2b* does produce equivalent models:

THEOREM 1. *For all K, w, v, and ϕ, $K, w, v \models \phi$ iff $k2b(K), w, v \models \phi$.*

Our second concern is whether $k2b(K)$ satisfies all the conditions required by §2: Worldview Monotonicity, Worldview Equality, Worldview Closure, Says Transparency, and Belief Hand-off. If a belief model B does satisfy these conditions, then B is *well-formed*. And modal model K is well-formed if it satisfies all the conditions required by §3: Accessibility Equality, IT, ID, F2, H, and WSF. Construction *k2b* does, indeed, produce well-formed belief models:

PROPOSITION 2. *For all well-formed modal models K, belief model $k2b(K)$ is well-formed.*

We might wonder whether there is a construction that can soundly transform belief models into Kripke models. Consider trying to transform the following belief model B into a Kripke model:

> B has a single world w and a proposition (i.e., a nullary relation) X, such that, for all v, it holds that $B, w, v \not\models X$. Suppose that principal p's worldview contains X—i.e., for all v, it holds that $X \in \omega(w, p, v)$—and that p's worldview does not contain false. By the semantics of says, it holds that $B, w, v \models p$ says X.

When transforming B to a Kripke model K, what edges could we put in $\leq_p$? There are only two choices: $\leq_p$ could be empty, or $\leq_p$ could contain the single edge (w, w). If $\leq_p$ is empty, then p is compromised, hence p says false. That contradicts our assumption that false is not in p's worldview. If $w \leq_p w$, then for w' and w'' such that $w \leq w' \leq_p w''$, it does not hold that $K, w'', v \models X$, because w and w'' can only be instantiated as w, and because $B, w, v \not\models X$. Hence p does not say X. That contradicts our assumption that X is in p's worldview. So we cannot construct an accessibility relation $\leq_p$ that causes the resulting Kripke semantics to preserve validity of formulas from the belief semantics.

There is, therefore, no construction that can soundly transform belief models into Kripke models—unless, perhaps, the set of worlds is permitted to change. We conjecture that it is possible to synthesize a new set of possible worlds, and equivalence relations on them, yielding a Kripke model that preserves validity of formulas from the belief model.

5. PROOF SYSTEM

FOCAL's derivability judgment is written $\Gamma \vdash \phi$ where Γ is a set of formulas called the *context*.[15] As is standard, we write $\vdash \phi$ when Γ is the empty set. In that case, ϕ is a *theorem*. We write Γ, ϕ to denote $\Gamma \cup \{\phi\}$.

Figure 5 presents the proof system. In it, $\phi[\tau/x]$ denotes capture-avoiding substitution of τ for x in ϕ. The first-order fragment of the proof system is routine (e.g., [38, 45, 49]).[16] SAYS-LRI, SAYS-LI, and SAYS-RI use notation τ says Γ, which means that τ says all the formulas in set Γ. Formally, τ says Γ is defined as $\{\tau$ says $\phi \mid \phi \in \Gamma\}$.

SAYS-LRI corresponds [27] to standard axiom K along with rule N from epistemic logic; SAYS-RI, to standard axiom 4; and SAYS-LI, to the converse $C4$ [3, 10] of 4:

$$K: \quad \vdash (p \text{ says } (\phi \Rightarrow \psi)) \Rightarrow (p \text{ says } \phi) \Rightarrow (p \text{ says } \psi),$$
$$N: \quad \text{From } \vdash \phi \text{ infer } \vdash p \text{ says } \phi,$$
$$4: \quad \vdash (p \text{ says } \phi) \Rightarrow (p \text{ says } (p \text{ says } \phi)),$$
$$C4: \quad \vdash (p \text{ says } (p \text{ says } \phi)) \Rightarrow (p \text{ says } \phi).$$

K and SAYS-LRI mean that *modus ponens* applies inside says. They correspond to Worldview Closure. Because of SAYS-LRI and IMP-I, the deduction theorem holds for FOCAL [24]. $C4$ and 4, along with SAYS-LI and SAYS-RI, mean that p says (p says ϕ) is equivalent to p says ϕ; they correspond to Says Transparency in the belief semantics. In the Kripke semantics, SAYS-RI corresponds to IT; and SAYS-LI,

[14] Another solution would be to stipulate that every principal p can be named by a term $\hat{p}$ in the syntax.

[15] These formulas are *localized hypotheses*, which the proof system uses instead of the hypothetical judgments found in natural deduction systems. Similar to the left-hand side Γ of a sequent $\Gamma \Longrightarrow \Delta$, the localized hypotheses are assumptions being used to derive right-hand side Δ. Unlike a sequent, Γ is a set, not a sequence.

[16] Under the usual constructive definition of $\neg\phi$ as $\phi \Rightarrow$ false, rules NOT-I and NOT-E are merely admissible rules and could be eliminated from the proof system.

$$\frac{}{\Gamma, \phi \vdash \phi}\ \text{HYP} \qquad \frac{\Gamma \vdash \phi}{\Gamma, \psi \vdash \phi}\ \text{WEAK} \qquad \frac{}{\Gamma \vdash \mathsf{true}}\ \text{TRUE-I} \qquad \frac{\Gamma \vdash \mathsf{false}}{\Gamma \vdash \phi}\ \text{FALSE-E} \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\ \text{AND-I} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ \text{AND-LE}$$

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ \text{AND-RE} \qquad \frac{\Gamma \vdash \phi_1}{\Gamma \vdash \phi_1 \vee \phi_2}\ \text{OR-LI} \qquad \frac{\Gamma \vdash \phi_2}{\Gamma \vdash \phi_1 \vee \phi_2}\ \text{OR-RI} \qquad \frac{\Gamma \vdash \phi_1 \vee \phi_2 \quad \Gamma, \phi_1 \vdash \psi \quad \Gamma, \phi_2 \vdash \psi}{\Gamma \vdash \psi}\ \text{OR-E} \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}\ \text{IMP-I}$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \phi \Rightarrow \psi}{\Gamma \vdash \psi}\ \text{IMP-E} \qquad \frac{\Gamma, \phi \vdash \mathsf{false}}{\Gamma \vdash \neg\phi}\ \text{NOT-I} \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \neg\phi}{\Gamma \vdash \mathsf{false}}\ \text{NOT-E} \qquad \frac{\Gamma \vdash \phi \quad x \notin FV(\Gamma)}{\Gamma \vdash (\forall\, x : \phi)}\ \text{FORALL-I} \qquad \frac{\Gamma \vdash (\forall\, x : \phi)}{\Gamma \vdash \phi[\tau/x]}\ \text{FORALL-E}$$

$$\frac{\Gamma \vdash \phi[\tau/x]}{\Gamma \vdash (\exists\, x : \phi)}\ \text{EXISTS-I} \qquad \frac{\Gamma \vdash (\exists\, x : \phi) \quad \Gamma, \phi \vdash \psi \quad x \notin FV(\Gamma, \psi)}{\Gamma \vdash \psi}\ \text{EXISTS-E} \qquad \frac{}{\Gamma \vdash \tau = \tau}\ \text{EQ-R} \qquad \frac{\Gamma \vdash \tau_1 = \tau_2}{\Gamma \vdash \tau_2 = \tau_1}\ \text{EQ-S}$$

$$\frac{\Gamma \vdash \tau_1 = \tau_2 \quad \Gamma \vdash \tau_2 = \tau_3}{\Gamma \vdash \tau_1 = \tau_3}\ \text{EQ-T} \qquad \frac{\Gamma \vdash \tau_i = \tau_i'}{\Gamma \vdash f(\tau_1, \ldots, \tau_n) = f(\tau_1', \ldots, \tau_n')}\ \text{EQ-FUN} \qquad \frac{\Gamma \vdash r(\tau_1, \ldots, \tau_n) \quad \Gamma \vdash \tau_i = \tau_i'}{\Gamma \vdash r(\tau_1', \ldots, \tau_n')}\ \text{EQ-REL}$$

$$\frac{\Gamma \vdash \phi}{\tau\ \mathsf{says}\ \Gamma \vdash \tau\ \mathsf{says}\ \phi}\ \text{SAYS-LRI} \qquad \frac{\Gamma \vdash \tau\ \mathsf{says}\ \phi}{\tau\ \mathsf{says}\ \Gamma \vdash \tau\ \mathsf{says}\ \phi}\ \text{SAYS-LI} \qquad \frac{\tau\ \mathsf{says}\ \Gamma \vdash \phi}{\tau\ \mathsf{says}\ \Gamma \vdash \tau\ \mathsf{says}\ \phi}\ \text{SAYS-RI} \qquad \frac{\Gamma \vdash \tau_2\ \mathsf{says}\ (\tau_1\ \mathsf{speaksfor}\ \tau_2)}{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_2}\ \text{SF-I}$$

$$\frac{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_2 \quad \Gamma \vdash \tau_1\ \mathsf{says}\ \phi}{\Gamma \vdash \tau_2\ \mathsf{says}\ \phi}\ \text{SF-E} \qquad \frac{}{\Gamma \vdash \tau\ \mathsf{speaksfor}\ \tau}\ \text{SF-R} \qquad \frac{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_2 \quad \Gamma \vdash \tau_2\ \mathsf{speaksfor}\ \tau_3}{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_3}\ \text{SF-T}$$

Figure 5: FOCAL derivability judgment

to ID. By including rules corresponding to 4 and $C4$, it is not our intent to argue that those axioms are necessary in authorization logics (which is debatable); rather, our intent is just to show how to support them.

SF-I corresponds to hand-off (1). SF-E uses speaksfor to deduce beliefs. SF-R and SF-T state that speaksfor is reflexive and transitive.

The usual sequent calculus structural rules of contraction, substitution and exchange are all admissible. But weakening (our rule WEAK) is not admissible: it must be directly included in the proof system, because the conclusions of SAYS-{LRI,LI,RI} capture their entire context Γ inside says.

5.1 Soundness

Our first soundness theorem for FOCAL states that if ϕ is provable from assumptions Γ, and that if a belief model validates all the formulas in Γ, then that model must also validate ϕ. Therefore, any provable formula is valid in the belief semantics:

THEOREM 2. *If $\Gamma \vdash \phi$ and $B, w, v \models \Gamma$, then $B, w, v \models \phi$.*

We have mechanized the proof of this theorem in Coq. The result is, to our knowledge, the first proof of soundness for an authorization logic w.r.t. a belief semantics. The proof of theorem 2 relies on the following proposition, which states monotonicity of validity w.r.t. $\leq$:

PROPOSITION 3. *If $B, w, v \models \phi$ and $w \leq w'$ then $B, w', v \models \phi$.*

The proof of it is also mechanized in Coq.

Our second soundness theorem for FOCAL states that any provable formula is valid in the Kripke semantics:

THEOREM 3. *If $\Gamma \vdash \phi$ and $K, w, v \models \Gamma$, then $K, w, v \models \phi$.*

The proof of that theorem relies on proposition 1 (monotonicity of the Kripke semantics). We also have mechanized the proofs of theorem 3 and proposition 1 in Coq. Those proofs currently use one additional axiom about the interpretation of principals: If the interpretation of a term at a world is principal p, then all other worlds must interpret that term as a principal equivalent to p. So a term must always be interpreted as the same principal. Formally, for all τ and w, if $\mu(w, \tau) \in P$ then, for all w', it must hold that $\mu(w', \tau) \in P$ and $\mu(w, \tau) \doteq \mu(w', \tau)$. We believe that, with additional work, this axiom can weakened to a statement that follows from the definition of the Kripke semantics.

5.2 State in distributed systems

FOCAL has essentially the same proof system as NAL, but there are a few differences. The most important is that we deliberately designed the FOCAL proof system such that its theory differs in one important way from the equivalent fragment of NAL's proof system. (That is, the fragment of NAL without *restricted delegation*, *subprincipals*, and *intensional group principals* [42].) We discuss our motivation for this change, next.

There are two standard ways of "importing" beliefs into a principal's worldview. The first is rule N from §5, also known as the rule of Necessitation: from $\vdash \phi$, infer $\vdash p$ says ϕ. The second is an axiom known as Unit: $\vdash \phi \Rightarrow (p\ \mathsf{says}\ \phi)$. Though superficially similar, it is well-known that Necessitation and Unit lead to different theories. Abadi [3] explores some of the proof-theoretic differences, particularly some of the surprising consequences of Unit in classical authorization logic. In the example below, we focus on one difference that does not seem to have been explored in constructive authorization logic:

EXAMPLE 3. *Machines M_1 and M_2 execute processes P_1 and P_2, respectively. M_1 has a register R. Let Z be a proposition representing "register R is currently set to zero." According to Unit, $\vdash Z \Rightarrow (P_1\ \mathsf{says}\ Z)$ and $\vdash Z \Rightarrow (P_2\ \mathsf{says}\ Z)$. The former means that a process on a machine knows the current contents of a register on that machine; the latter means that a process on a different machine must also know*

the current contents of the register. But according to Necessitation, if $\vdash Z$ *then* $\vdash P_1$ says Z *and* $\vdash P_2$ says Z*. Only if* R *is guaranteed to be constant—i.e., it can never at any time be anything other than zero—must the two processes say so.*

Unit, therefore, is appropriate when propositions (or relations or functions) represent global state upon which all principals are guaranteed to agree. But when propositions represent local state that could be unknown to some principals, Unit would arguably be an invalid axiom. A countermodel demonstrating Unit's invalidity is easy to construct—for example, stipulate a world w at which Z holds, and let P_1's worldview contain Z but P_2's worldview not contain Z. That countermodel doesn't apply to Necessitation, because Z is not a theorem in it, therefore the principals may disagree on Z's validity.

Prior work has objected to Unit for other reasons (cf. §6), but not for this difference between local and global state. We are unaware of any authorization logic that rejects Necessitation, which is widely accepted along with axiom K (cf. §5) in *normal modal logic* [27].

FOCAL is designed for reasoning about state in distributed systems, where principals (such as machines) may have local state, and where global state does not necessarily exist—the reading at a clock, for example, is not agreed upon by all principals. So Unit would be invalid for FOCAL principals; Necessitation is the appropriate choice. We therefore include Necessitation in FOCAL in the form of rule SAYS-LRI. Having that rule in our proof system is equivalent to having both Necessitation and K in a natural-deduction proof system [27, p. 214, where SAYS-LRI is called LR].

Similarly, NAL principals do not necessarily agree upon global state. NAL does include Necessitation as an inference rule and does not include Unit as an axiom. However, NAL permits Unit to be derived as a theorem:[17]

$$\dfrac{\dfrac{[\phi]^1}{p \text{ says } \phi}\ \text{NAL-SAYS-I}}{\phi \Rightarrow p \text{ says } \phi}\ \text{NAL-IMP-I}_1$$

NAL's proof system is, therefore, arguably unsound w.r.t. our belief semantics: there is a formula (Unit) that is a theorem of the system but that is not semantically valid.

NAL extends CDD's proof system [2], so we might suspect that CDD is also unsound w.r.t. our semantics. And it is. However, CDD has been proved sound w.r.t. a *lax logic* semantics [19]. That semantics employs a different intuition about says than NAL. CDD understands p says ϕ to mean "when combining the [statement ϕ] that the [guard] believes with those that [p] contributes, the [guard] can conclude ϕ... the [guard's] participation is left implicit" [2, p. 13]. In other words, the guard's beliefs are imported into p's beliefs at each world. That results in a different meaning of says than FOCAL or NAL employs.

FOCAL's proof system instead prohibits derivation of Unit: Unit is invalid in our semantics, and our proof system is sound w.r.t. our semantics, so it's impossible for our proof system to derive Unit. FOCAL therefore seem appropriate for reasoning about state in distributed systems.

[17]Rules NAL-IMP-I and NAL-SAYS-I can be found in [42]. The brackets around ϕ at the top of the proof tree indicate that it is used as a hypothesis [49]. The appearance of "1" as a super- and subscript indicate where the hypothesis is introduced and cancelled.

6. RELATED WORK

FOCAL has the first formal belief semantics of any authorization logic. To our knowledge, belief semantics have been used in only one other authorization logic, and that logic—NAL [42]—has only an informal semantics based on worldviews.

But many of the pieces of FOCAL, including its semantics and proof system, are naturally derived from previous work. We summarize here what we borrowed vs. what we invented; the main body of the paper contains detailed citations. FOCAL's belief semantics is a standard first-order constructive semantics, but the addition of worldviews to interpret says and speaksfor is novel (with the exception of NAL, which used worldviews informally). FOCAL's Kripke semantics for everything except speaksfor is likewise standard, and its frame conditions (except H and WSF) are already well-known in constructive modal logic, but the application of IT and ID to authorization logic seems to be novel. FOCAL's proof system, excluding says and speaksfor, is a straightforward first-order constructive proof system. The fragment for says is our own adaptation of modal-logic natural-deduction rules for the $\Box$ connective. The fragment for speaksfor is a straightforward formalization of the standard definitions and axioms used in many authorization logics.

Semantic structures similar to our belief models have been investigated in the context of epistemic logic [13, 15, 37]. Konolige [30] proves an equivalence result for classical propositional logic similar to our theorem 1.

Garg and Abadi [19] give a Kripke semantics for a logic they call ICL, which could be regarded as a propositional fragment of FOCAL. The ICL semantics of says, however, uses *invisible* worlds to permit principals to be oblivious to the truth of formulas at some worlds. That makes Unit (§5.2) valid in ICL, whereas Unit is invalid in FOCAL.

Garg [18] studies the proof theory of a logic called DTL_0, and gives a Kripke semantics that uses both invisible worlds and *fallible* worlds, at which false is permitted to be valid. Instead of Unit, it uses the axiom p says $((p \text{ says } \phi) \Rightarrow \phi)$. That axiom is unsound in FOCAL. DTL_0 does not have a speaksfor connective.

Genovese et al. [22] study several uses for Kripke semantics with an authorization logic they call BL_{sf}, which also could be regarded as a propositional fragment of FOCAL. They show how to generate evidence for why an access should be denied, how to find all logical consequences of an authorization policy, and how to determine which additional credentials would allow an access. However, the Kripke semantics of BL_{sf} differs from FOCAL's in its interpretation of both says and speaksfor, so the results of Genovese et al. are not immediately applicable to FOCAL.

Garg and Pfenning [20] prove *non-interference* properties for a first-order constructive authorization logic. Such properties mean that one principal's beliefs cannot interfere with another principal's beliefs unless there is some trust relationship between those principals. Abadi [2] also proves such a property for dependency core calculus (DCC), which is the basis of authorization logic CDD. We conjecture that similar properties could be proved for FOCAL.

One of the more intriguing consequences of our semantics is that says is not a *monad* [36]. Since Abadi's invention of CDD [2], says is frequently assumed to satisfy the *monad laws*, which include Unit. In our semantics, however, Unit

is invalid. The monad laws also include a law named Bind, which turns out to be invalid in our semantics as well. We don't know whether rejecting the monad laws will have any practical impact on FOCAL. But the seminal authorization logic, ABLP [4], didn't adopt the monad laws. Likewise, Garg and Pfenning [21] reject Unit in their authorization logic BL_0; they demonstrate that Unit leads to counterintuitive interpretations of some formulas involving delegation. And Abadi [1] notes that Unit "should be used with caution (if at all)," suggesting that it be replaced with the weaker axiom $(p \text{ says } \phi) \Rightarrow (q \text{ says } p \text{ says } \phi)$. Genovese et al. [22] carry out that suggestion. So in rejecting the monad laws, FOCAL is at least in good company.

7. CONCLUDING REMARKS

This work began with the idea of giving a Kripke semantics to NAL. Proving soundness—at first on paper, not in Coq—turned out to be surprising, because Unit is semantically invalid but derivable in NAL (§5.2). The complexity of the resulting Kripke semantics motivated us to seek a simpler semantics. We were inspired by the informal worldview semantics of the NAL rationale [42] and elaborated that into our belief semantics (§2). In future work, we plan to upgrade FOCAL to handle NAL's advanced features, including *intensional group principals*.

Mechanizing the proofs of soundness in Coq was frequently rewarding. It exposed several bugs (in either our proof system or our semantics) and gave us high confidence in the correctness of the result. We expect further benefits, too. Other researchers can now use our formalization as a basis for mechanizing results about authorization logics. And from the formalization of the FOCAL proof system in Coq, we could next extract a *verified theorem checker*. It would input a proof of a FOCAL formula, expressed in the FOCAL proof system, and output whether the proof is correct. Coq would verify that the checker correctly implements the FOCAL proof system. After FOCAL is upgraded to handle all of NAL's features, the resulting theorem checker could replace the current Nexus [44] theorem checker, which is implemented in C. A verified theorem checker would arguably be more trustworthy than the C implementation, thus increasing the trustworthiness of the operating system.

Our goal was to increase the trustworthiness of authorization logics, hence our concentration on soundness results. Another worthwhile goal would to be increase the utility of authorization logics, and toward that end we could investigate the *completeness* of FOCAL: are all valid formulas provable? A few authorization logics—ICL [19], DTL_0 [18], and BL_{sf} [22]—do have completeness results for Kripke semantics; however, none of those is immediately applicable to FOCAL.[18] We leave adaptation of them as future work.

8. REFERENCES

[1] M. Abadi. Logic in access control. In *Proc. IEEE Symposium on Logic in Computer Science (LICS)*, pages 228–233, 2003.

[2] M. Abadi. Access control in a core calculus of dependency. *Electronic Notes in Theoretical Computer Science*, 172:5–31, Apr. 2007.

[3] M. Abadi. Variations in access control logic. In *Proc. Conference on Deontic Logic in Computer Science (DEON)*, pages 96–109, 2008.

[4] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, Sept. 1993.

[5] A. W. Appel and E. W. Felten. Proof-carrying authentication. In *Proc. ACM Conference on Computer and Communications Security (CCS)*, pages 52–62, 1999.

[6] L. Bauer, S. Garriss, J. M. McCune, M. K. Reiter, J. Rouse, and P. Rutenbar. Device-enabled authorization in the Grey system. In *Proc. Information Security Conference (ISC)*, pages 431–445, 2005.

[7] M. Y. Becker, C. Fournet, and A. D. Gordon. SecPAL: Design and semantics of a decentralized authorization language. *Journal of Computer Security*, 18(4):619–665, 2010.

[8] M. Y. Becker and P. Sewell. Cassandra: Distributed access control policies with tunable expressiveness. In *Proc. IEEE Workshop on Policies for Distributed Systems and Networks (POLICY)*, pages 159–168, 2004.

[9] J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *Int'l Journal of Information Security*, 6(2–3):133–151, 2007.

[10] B. F. Chellas. *Modal Logic: An Introduction*. Cambridge University Press, Cambridge, United Kingdom, 1980.

[11] A. Cirillo, R. Jagadeesan, C. Pitcher, and J. Riely. Do As I SaY! Programmatic access control with explicit identities. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 16–30, 2007.

[12] J. DeTreville. Binder, a logic-based security language. In *IEEE Symposium on Security and Privacy*, pages 105–113, 2002.

[13] R. A. Eberle. A logic of believing, knowing and inferring. *Synthese*, 26:356–382, 1974.

[14] W. B. Ewald. Intuitionistic tense and modal logic. *Journal of Symbolic Logic*, 51(1):166–179, 1986.

[15] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning About Knowledge*. MIT Press, Cambridge, Massachusetts, 1995.

[16] G. Fischer Servi. Semantics for a class of intuitionistic modal calculi. In M. L. D. Chiara, editor, *Italian Studies in the Philosophy of Science*, pages 59–72. D. Riedel Publishing Company, Dordrecht, Holland, 1981.

[17] C. Fournet, A. D. Gordon, and S. Maffeis. A type discipline for authorization policies. In *Proc. European Symposium on Programming (ESOP)*, pages 141–156, 2005.

[18] D. Garg. Principal-centric reasoning in constructive authorization logic. In *Workshop on Intuitionistic Modal Logic and Applications (IMLA)*, 2008.

[19] D. Garg and M. Abadi. A modal deconstruction of

[18] ICL uses a *lax logic* semantics that is incompatible with FOCAL's definition of says. DTL_0 uses a Kripke semantics with *invisible* and *fallible* worlds, and it omits the speaksfor connective. And BL_{sf} encodes speaksfor as a first-order relation, rather than defining it with accessibility relations, and it does not provide a weak speaksfor semantics.

access control logics. In *Proc. Conference on Foundations of Software Science and Computational Structures (FOSSACS)*, pages 216–230, 2008.

[20] D. Garg and F. Pfenning. Non-interference in constructive authorization logic. In *Proc. IEEE Computer Security Foundations Workshop (CSFW)*, pages 283–296, 2006.

[21] D. Garg and F. Pfenning. Stateful authorization logic: Proof theory and a case study. In *Proc. Conference on Security and Trust Management (STM)*, pages 210–225, 2010.

[22] V. Genovese, D. Garg, and D. Rispoli. Labeled sequent calculi for access control logics: Countermodels, saturation and abduction. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 139–153, 2012.

[23] Y. Gurevich and I. Neeman. DKAL: Distributed-knowledge authorization language. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 149–162, 2008.

[24] R. Hakli and S. Negri. Does the deduction theorem fail for modal logic? *Synthese*, 187(3):849–867, 2012.

[25] J. Hintikka. *Knowledge and Belief*. Cornell University Press, Ithaca, New York, 1962.

[26] J. Howell. *Naming and Sharing Resources across Administrative Domains*. PhD thesis, Dartmouth College, 2000.

[27] G. E. Hughes and M. J. Cresswell. *A New Introduction to Modal Logic*. Routledge, London, 1996.

[28] L. Jia, J. A. Vaughan, K. Mazurak, J. Zhao, L. Zarko, J. Schorr, and S. Zdancewic. AURA: A programming language for authorization and audit. In *Proc. ACM Int'l Conference on Functional Programming (ICFP)*, pages 27–38, 2008.

[29] T. Jim. SD3: A trust management system with certified evaluation. In *IEEE Symposium on Security and Privacy*, pages 106–115, 2001.

[30] K. Konolige. *A Deduction Model of Belief*. Morgan Kaufmann, Los Altos, California, 1986.

[31] S. Kripke. A semantical analysis of modal logic I: Normal modal propositional calculi. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 9:67–96, 1963. Announced in *Journal of Symbolic Logic*, 24:323, 1959.

[32] B. Lampson, M. Abadi, M. Burrows, and E. Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, Nov. 1992.

[33] C. Lesniewski-Laas, B. Ford, J. Strauss, R. Morris, and M. F. Kaashoek. Alpaca: extensible authorization for distributed services. In *Proc. ACM Conference on Computer and Communications Security (CCS)*, pages 432–444, 2007.

[34] N. Li, B. N. Grosof, and J. Feigenbaum. A practically implementable and tractable delegation logic. In *IEEE Symposium on Security and Privacy*, pages 27–42, 2000.

[35] N. Li, J. C. Mitchell, and W. H. Winsborough. Design of a role-based trust-management framework. In *IEEE Symposium on Security and Privacy*, pages 114–130, 2002.

[36] E. Moggi. Notions of computation and monads. *Journal of Information and Computation*, 93(1):55–92, July 1991.

[37] R. Moore and G. Hendrix. Computational models of beliefs and the semantics of belief structures. Technical Note 187, SRI International, 1979.

[38] S. Negri and J. von Plato. Sequent calculus in natural deduction style. *Journal of Symbolic Logic*, 66:1803–1816, 2001.

[39] R. Parikh. Knowledge and the problem of logical omniscience. In *Proc. Int'l Symposium on Methodologies for Intelligent Systems (ISMIS)*, pages 432–439, 1987.

[40] A. Pimlott and O. Kiselyov. Soutei, a logic-based trust-management system. In *Proc. Functional and Logic Programming Symposium (FLOPS)*, pages 130–145, 2006.

[41] G. Plotkin and C. Stirling. A framework for intuitionistic modal logics. In *Proc. Conference on Theoretical Aspects of Reasoning about Knowledge (TARK)*, pages 399–406, 1986.

[42] F. B. Schneider, K. Walsh, and E. G. Sirer. Nexus authorization logic (NAL): Design rationale and applications. *ACM Transactions on Information and System Security*, 14(1):8:1–28, June 2011.

[43] A. K. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.

[44] E. G. Sirer, W. de Bruijn, P. Reynolds, A. Shieh, K. Walsh, D. Williams, and F. B. Schneider. Logical attestation: An authorization architecture for trustworthy computing. In *Proc. ACM Symposium on Operating Systems Principles (SOSP)*, pages 249–264, 2011.

[45] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, Amsterdam, 2006.

[46] R. Stalnaker. The problem of logical omniscience, I. *Synthese*, 89:425–440, 1991.

[47] A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics: Volume I*, volume 121 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, Amsterdam, 1988.

[48] A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics: Volume II*, volume 123 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, Amsterdam, 1988.

[49] D. van Dalen. *Logic and Structure*. Springer, Berlin, fourth edition, 2004.

[50] D. Wijesekera. Constructive modal logics I. *Annals of Pure and Applied Logic*, 50(3):271–301, Dec. 1990.

[51] E. Wobber, M. Abadi, M. Burrows, and B. Lampson. Authentication in the Taos operating system. *ACM Transactions on Computer Systems*, 12(1):3–32, Feb. 1994.

APPENDIX

A. PROOFS

Proposition 1.

If $K, w, v \models \phi$ and $w \leq w'$ then $K, w', v \models \phi$.

Proof. By structural induction on ϕ. This proof has been mechanized in Coq. □

Theorem 1.

For all K, w, v, and ϕ, it holds that $K, w, v \models \phi$ iff $k2b(K), w, v \models \phi$.

Proof. First, we show the forward direction: $K, w, v \models \phi$ implies $k2b(K), w, v \models \phi$. All of the cases except says and speaksfor are straightforward, because those are the only two cases where the interpretation of formulas differs in the two semantics.

- Case $\phi = \tau$ says ψ. Suppose $K, w, v \models \tau$ says ψ. By the definition of *k2b*, formula $\psi \in \omega(w, \mu(\tau), v)$. By the belief semantics of says, it must hold that $k2b(K), w, v \models \tau$ says ψ.
- Case $\phi = \tau$ speaksfor τ'. Assume $K, w, v \models \tau$ speaksfor τ'. We need to show that, for all $w' \geq w$, it holds that $\omega(w', \mu(\tau), v) \subseteq \omega(w', \mu(\tau'), v)$. So let w' and ψ be arbitrary such that $w' \geq w$ and $\psi \in \omega(w', \mu(\tau), v)$, and we'll show that $\psi \in \omega(w', \mu(\tau'), v)$. By the definition of *k2b*, it holds that $K, w', v \models \tau$ says ψ. Note that, by proposition 1 and our original assumption, we have that $K, w', v \models \tau$ speaksfor τ'. From those last two facts, and from the Kripke semantics of says and speaksfor, it follows that $K, w', v \models \tau'$ says ψ. By the definition of *k2b*, it therefore holds that $\psi \in \omega(w', \mu(\tau'), v)$.

Second, we show the backward direction: $K, w, v \models \phi$ is implied by $k2b(K), w, v \models \phi$. Again, all of the cases except says and speaksfor are straightforward, because those are the only two cases where the interpretation of formulas differs in the two semantics.

- Case $\phi = \tau$ says ψ. Suppose $k2b(K), w, v \models \tau$ says ψ. By the belief semantics of says, we have that $\psi \in \omega(w, \mu(\tau), v)$. By the definition of *k2b*, it holds that $K, w, v \models \tau$ says ψ.
- Case $\phi = \tau$ speaksfor τ'. Assume $k2b(K), w, v \models \tau$ speaksfor τ'. By the belief semantics of speaksfor, we have that, for all $w' \geq w$, it holds that $\omega(w', \mu(\tau), v) \subseteq \omega(w', \mu(\tau'), v)$. Let w' be w. Then $\omega(w, \mu(\tau), v) \subseteq \omega(w, \mu(\tau'), v)$. By the definitions of *k2b* and subset, it follows that, for all ϕ, if $K, w, v \models \tau$ says ϕ then $K, w, v \models \tau'$ says ϕ. By WSF, we therefore have that $K, w, v \models \tau$ speaksfor τ'.

□

Proposition 2.

For all well-formed modal models K, belief model $k2b(K)$ is well-formed.

Proof. Let $B = k2b(K)$. For B to be well-formed it must satisfy several conditions, which were defined in §2. We now show that these hold for any such B constructed by *k2b*.

1. Worldview Monotonicity. Assume $w \leq w'$ and $\phi \in \omega(w, p, v)$. By the latter assumption and the definition of *k2b*, we have that $K, w, v \models \hat{p}$ says ϕ. From proposition 1, it follows that $K, w', v \models \hat{p}$ says ϕ. By the definition of *k2b*, it then holds that $\phi \in \omega(w', p, v)$. Therefore $\omega(w, p, v) \subseteq \omega(w', p, v)$.
2. Worldview Equality. Assume $p \doteq p'$. Then by Accessibility Equality, $\leq_p$ equals $\leq_{p'}$. By the Kripke semantics of says, it follows that $K, w, v \models p$ says ϕ iff $K, w, v \models p'$ says ϕ. By the definition of *k2b*, therefore, $\omega(w, p, v) = \omega(w, p', v)$.
3. Worldview Closure. Assume $\Gamma \subseteq \omega(w, p, v)$ and $\Gamma \models \phi$, that is, ϕ is a logical consequence of Γ in belief structure B. By the definition of *k2b*, we have $\omega(w, p, v) = \{\phi \mid K, w, v \models \hat{p}$ says $\phi\}$. So for all $\psi \in \Gamma$, it holds that $K, w, v \models \hat{p}$ says ψ. By the Kripke semantics of says, it follows that for all w' and w'' such that $w \leq w' \leq_p w''$, it holds that $K, w'', v \models \psi$. Thus $K, w'', v \models \Gamma$. So $k2b(K), w'', v \models \Gamma$ by theorem 1. By our initial assumption that $\Gamma \models \phi$, it follows that $k2b(K), w'', v \models \phi$. Again applying theorem 1, we have that $K, w'', v \models \phi$. By the Kripke semantics of says, it follows that $K, w, v \models \hat{p}$ says ϕ. Therefore, by the definition of *k2b*, we have $\phi \in \omega(w, p, v)$.
4. Says Transparency. We prove the "iff" by proving both directions independently.

   ($\Rightarrow$) Assume $\phi \in \omega(w, p, v)$. By the definition of *k2b*, it holds that $K, w, v \models \hat{p}$ says ϕ. From IT and F2, it follows that $K, w, v \models \hat{p}$ says ($\hat{p}$ says ϕ). By the definition of *k2b*, therefore, ($\hat{p}$ says ϕ) $\in \omega(w, p, v)$.

   ($\Leftarrow$) Assume ($\hat{p}$ says ϕ) $\in \omega(w, p, v)$. By the definition of *k2b*, it holds that $K, w, v \models \hat{p}$ says ($\hat{p}$ says ϕ). From ID, it follows that $K, w, v \models \hat{p}$ says ϕ. By the definition of *k2b*, therefore, $\phi \in \omega(w, p, v)$.
5. Belief Hand-off. We actually prove a stronger result—an "iff" rather than just an "if". By the definitions of subset and *k2b*, we have that $\omega(w, p, v) \subseteq \omega(w, q, v)$ holds iff for all ϕ, if $K, w, v \models \hat{p}$ says ϕ then $K, w, v \models \hat{q}$ says ϕ. By WSF, that holds iff $K, w, v \models \hat{p}$ speaksfor $\hat{q}$. By the fact below, that holds iff $K, w, v \models \hat{q}$ says ($\hat{p}$ speaksfor $\hat{q}$). By the definition of *k2b*, that holds iff $\hat{q}$ speaksfor $\hat{p} \in \omega(w, q, v)$.

   Fact: in the Kripke semantics, $\models \hat{q}$ says ($\hat{p}$ speaksfor $\hat{q}$) $\iff$ $\hat{p}$ speaksfor $\hat{q}$. The proof of that fact has been mechanized in Coq.

□

Theorem 2.

If $\Gamma \vdash \phi$ and $B, w, v \models \Gamma$, then $B, w, v \models \phi$.

Proof. By induction on the derivation of $\Gamma \vdash \phi$. This proof has been mechanized in Coq. □

Theorem 3.

If $\Gamma \vdash \phi$ and $K, w, v \models \Gamma$, then $K, w, v \models \phi$.

Proof. By induction on the derivation of $\Gamma \vdash \phi$. This proof has been mechanized in Coq. □

Proposition 3.

If $B, w, v \models \phi$ and $w \leq w'$ then $B, w', v \models \phi$.

Proof. By structural induction on ϕ. This proof has been mechanized in Coq. □