A constructive conditional logic for access control: a completeness result

Valerio Genovese (1), Laura Giordano (2),
Valentina Gliozzi (3), and Gian Luca Pozzato (3)

(1) Computer Science and Communications Research Unit
University of Luxembourg - Walferdange, Luxembourg
e-mail: valerio.genovese@uni.lu

(2) Dipartimento di Informatica - Università del Piemonte Orientale
Alessandria, Italy - e-mail: laura@mfn.unipmn.it

(3) Dipartimento di Informatica - Università degli Studi di Torino
Torino, Italy
e-mail: {gliozzi,pozzato}@di.unito.it

Abstract

In this paper we define a Intuitionistic Conditional Logic for Access Control (CC_{AC}). The logic is based on a conditional language allowing principals to be defined as arbitrary formulas. CC_{AC} is a intuitionistic conditional logic, which includes few uncontroversial axioms of access control logics. The paper provides an axiomatization and a Kripke model semantics for the logic CC_{AC} and proves that the axiomatization is sound and complete with respect to the semantics.

1 Introduction

The importance of constructive logics for access control is well-known in the literature. Abadi [1] describes alternative axiomatizations for an access control logic. He shows that an intuitionistic interpretation of the modality "says" allows to avoid unexpected conclusions that are derivable when "says" is given a classical interpretation.

In this paper we define an access control logics which combines intuitionistic logic with a conditional "says" modality. The says modality $\Box_A$ is labelled by a formula representing a principal, so that $\Box_A\phi$ has the intended meaning *principal* A *says that* ψ. The generality of this approach opens the way to the formalization of the so called boolean principals [2], that is, principals which are formed by boolean combination of atomic principals. However, in this paper we only focus on few uncontroversial axioms

of access control logics and leave for further work a precise analysis of the conditional axioms which enforce wanted properties for the boolean principals.

We define the conditional access logic CC_{AC} by defining an axiomatization and a Kripke semantics for the logic. The semantics extends the standard intuitionistic Kripke semantics with a collection of accessibility relations, each one associated with a says modality $\Box_A$. We prove that the axiomatization is sound and complete with respect to the semantics.

2 Axiom System

We define the language $\mathcal{L}$ of the logic CC_{AC}.

Let ATM be a set of atomic propositions. The formulas $\varphi \in \mathcal{L}$ are defined as follows:

$$\varphi ::= p \mid \bot \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \varphi \rightarrow \varphi \mid \Box_\varphi \varphi$$

where $p \in ATM$ and $\bot$ is a proposition which is always false.

The intended meaning of the formula $\Box_\varphi \psi$ is that *principal φ says that ψ*, namely, "the principal ϕ asserts or supports ψ" [2]. Although the principal ϕ is an arbitrary formula, in order to stress the fact that a formula is playing the role of a principal, we will denote it by $A, B, C, \ldots$ while we will use greek letters for arbitrary formulas. Thus, we will write $\Box_A \phi$ to mean that *principal A says that ψ*. Observe that conditional logic provides a natural generalization of multimodal logics by allowing modalities to be labelled by arbitrary formulas. In particular, the language above provides a generalization of the multimodal language in [2] where, in the formula $\Box_A \phi$, the modality A is an atomic principal rather than a formula.

The *axiom system* of the logic CC_AC contains the following axioms and inference rules:

$(TAUT)$ all tautologies of intuitionistic logic

(K) $\Box_A(\alpha \rightarrow \beta) \rightarrow \Box_A \alpha \rightarrow \Box_A \beta$

$(UNIT)$ $\alpha \rightarrow \Box_A \alpha$

(C) $\Box_A(\Box_A \alpha \rightarrow \alpha)$

(MP) If $\vdash \alpha$ and $\vdash \alpha \rightarrow \beta$ then $\vdash \beta$

$(RCEA)$ If $\vdash A \leftrightarrow B$ then $\vdash \Box_A \gamma \leftrightarrow \Box_B \gamma$

(RCK) If $\vdash \alpha \rightarrow \beta$ then $\vdash \Box_A \alpha \rightarrow \Box_A \beta$

The rule (MP) is modus ponens. (RCEA) and (RCK) are standard inference rules for conditional logics. (RCK) plays the role of the rule of Necessitation (if $\vdash A$ then $\vdash \Box_C A$) in modal/multimodal logic. The axiom (K) belongs to the axiomatization of all normal modal logics and it is derivable in "normal" conditional logics. (K) and (UNIT), are characterizing axioms of the access control logics ICL [2]. (C) is a slightly stronger axiom than (C4) of ICL. All the taultologies of intuitionistic logic are included, so that the resulting logic is an intuitionistic version of a conditional logic.

Given the axiomatization above, it is easy to see that the Deduction Theorem holds for CC_{AC}, namely, if $\vdash \alpha \rightarrow \beta$ then $\alpha \vdash \beta$, for all formulas α and β.

3 Semantics

The semantics of the logic is defined as follows.

Definition 3.1 *A CC_{AC} model has the form:*

$$M = (S, \leq, \{R_A\}, t_0, h)$$

where:

- *$S \neq \emptyset$ is a set of items called worlds;*
- *$\leq$ is a partial order over S;*
- *R_A is a binary relation on S associated with the formula A;*
- *$t_0 \in S$;*
- *h is an evaluation function $ATM \longrightarrow Pow(S)$ that associates to each atomic proposition p the set of worlds x in which p is true.*

We define the truth conditions of formulas with respect to worlds in a model M, by the relation $M, x \models \phi$, as follows. We use $[[\phi]]$ to denote $\{y \in S \mid M, y \models \phi\}$.

1. *$M, t \models q$ iff, for all s such that $t \leq s$, $s \in h(q)$*
2. *$M, t \models A \wedge B$ iff $M, t \models A$ and $M, t \models B$*
3. *$M, t \models A \vee B$ iff $M, t \models A$ or $M, t \models B$*
4. *$M, t \models A \rightarrow B$ iff for all s such that $t \leq s$ (if $M, s \models A$ then $M, s \models B$)*
5. *$M, t \models \neg A$ iff, for all s such that $t \leq s$, $M, s \not\models A$*
6. *$M, t \not\models \bot$*
7. *$M, t \models \Box_A \psi$ iff, for all s such that tR_As, $M, s \vDash \psi$.*

We say that ϕ is valid in a model M if $M, t_0 \models \phi$. We say that ϕ is valid *tout court (and write $\models \phi$) if ϕ is valid in every model. We extend the notion of validity to a set of formulas Γ in the obvious way: $M, t_0 \models \Gamma$ if $M, t_0 \models \psi$ for all $\psi \in \Gamma$. Last, we say that ϕ is a* logical consequence *of Γ (and write $\Gamma \models \phi$) if, for all models M, if $M, t_0 =\models \Gamma$, then $M, t_0 \models \phi$.*

The relations $\leq$ and R_A must satisfy the following conditions:

(a) $\forall t, s, z \in S$, if $s \leq t$ and tR_Az then sR_Az;

(b) $\forall t, s \in S$, if sR_At, then $t \leq s$;

(c) $\forall t, s \in S$, if sR_At, then tR_At;

(d) if $[[A]] = [[B]]$, then $R_A = R_B$,

Conditions (b) and (c) are, respectively, the semantic conditions associated with the axioms (UNIT) and (C), while condition (a) is needed to enforce the property that a formula true in a world t is also true in all worlds reachable from s by the relation $\leq$ (i.e., it is also true in all worlds s such that $t \leq s$). Condition (d) is the well-known condition for normality, claiming that the accessibility relation R_A is associated with the semantic interpretation of A.

Observe that, in the semantics above, the binary relation R_A plays the role of the selection function f, which is used in most formulation of conditional logics semantics. In particular, sR_At corresponds to $t \in f(A, s)$, and the conditions (a), (b), (c) and (d) above are indeed conditions on the selection function f, as usual in conditional logics.

4 Soundness and Completeness

In this section we prove that the axiomatization given above is sound and complete with respect to the semantics above. Soundness is straightforward.

Theorem 4.1 *The axiomatization of the logic CC_{AC} given in Section 2 is sound with respect to the Kripke semantics in Section 3: given a formula $A \in \mathcal{L}$, if $\Gamma \vdash A$, then $\Gamma \models A$*

Proof. It is easy to prove that each axiom is a valid formula and, for each inference rule, if the antecedent of the rule is a valid formula, the consequence of the rule is also a valid formula. ■

The completeness proof we present is based on the proof of completeness for for the Kripke semantics of intuitionistic logic in Troelstra and Van Dalen (see [3] section 6, page 87) and extends it to deal with the modalities $\Box_A$ in the language and, more precisely, with the interplay between the relation $\leq$ and the accessibility relations R_A associated with the modalities.

Definition 4.2 (Consistency) *Γ is consistent iff $\Gamma \nvdash \bot$. If Γ has an infinite number of formulas, we say that Γ is consistent iff there are no finite $\Gamma_0 \subset \Gamma$ such that $\Gamma_0 \vdash \bot$.*

Definition 4.3 (Saturation) *Let Γ be a set of well formed formulas, we say that Γ is saturated iff*

1. *Γ is consistent,*
2. *$\Gamma \vdash A \Rightarrow A \in \Gamma$*
3. *$\Gamma \vdash A \vee B \Rightarrow \Gamma \vdash A$ or $\Gamma \vdash B$*

Lemma 4.4 (Saturated Extensions) *Suppose $\Gamma \nvdash A$, then there is a saturated extension Γ^* such that $\Gamma^* \nvdash A$.*

The proof can be done by transfinite induction as in [3].

Lemma 4.5 *Let Γ be a set of formulas and let $\Delta = \{A : \Box_\mu A \in \Gamma\}$. If $\Delta \nvdash B$, then $\Gamma \nvdash \Box_U B$*

Proof. Suoopse there is a derivation of B from Δ. Then, there must be a finite set of formulas $\{A_1, \ldots, A_n\} \subseteq \Delta$ such that $\{A_1, \ldots, A_n\} \vdash B$. By the deduction theorem, $\vdash A_1 \wedge \ldots \wedge A_n \rightarrow B$. By (RCK) and (K), $\vdash \Box_U A_1 \wedge \ldots \wedge \Box_U A_n \rightarrow \Box_U B$. As $\Box_U A_i \in \Gamma$ for all $i = 1, n$, by modus ponens, $\Gamma \nvdash \Box_U B$. ■

Definition 4.6 (Canonical model construction) *Let Γ_0 be any saturated set of formulas. Then we define*

$$\mathbf{M} = (\mathbf{S}, \leq, \{\mathbf{R_A}\}, \mathbf{\Gamma_0}, \mathbf{h})$$

Such that

- *S is the set of all saturated $\Gamma \supseteq \Gamma_0$.*
- *$\Gamma_1 \leq \Gamma_2$ iff $\Gamma_1 \subseteq \Gamma_2$.*
- *$\Gamma_1 R_A \Gamma_2$ iff $\{\alpha \mid \Box_A \alpha \in \Gamma_1\} \subseteq \Gamma_2$*

Observe that in the above construction, $\Gamma_0 \in S$.

Lemma 4.7 *For all $\Gamma \in S$ and each wff formula A*

$$\Gamma \models A \Leftrightarrow A \in \Gamma$$

Proof. By induction on the complexity of A

- *Case 1.*: For A atomic the lemma holds by definition
- *Case 2.*: For $A \equiv B \wedge C$ immediate.
- *Case 3.*: For $A \equiv B \vee C$, then $\Gamma \models B \vee C \Leftrightarrow (\Gamma \models B \; or \; \Gamma \models C) \Leftrightarrow (B \in \Gamma \; or \; C \in \Gamma) \Leftrightarrow B \vee C \in \Gamma$ (by the saturation of Γ).
- *Case 4.*: Let $A \equiv B \rightarrow C$, and suppose $\Gamma \models B \rightarrow C$. Then for all saturated $\Gamma^{'} \supset \Gamma$ we have $\Gamma^{'} \models B \Rightarrow \Gamma' \models C$. Assume $\Gamma \nvdash B \rightarrow C$, then $\Gamma \cup \{B\} \nvdash C$; let $\Gamma^{'}$ be a saturated extension of $\Gamma \cup \{B\}$ such that $\Gamma^{'} \nvdash C$, then $\Gamma^{'} \models B$ but not $\Gamma^{'} \models C$ (induction hypotesis); this contradicts $\Gamma \models B \rightarrow C$, hence $\Gamma \vdash B \rightarrow C$. As γ is saturated, by condition 2 in Definition 4.3, $B \rightarrow C \in \Gamma$. The converse is trivial.
- *Case 5.*: Let $A \equiv \Box_A \phi$, and suppose $\Gamma \models \Box_A \phi$. Hence, for all Γ' such that $\Gamma R_A \Gamma'$, $\Gamma' \models \phi$. By inductive hypothesis, $\phi \in \Gamma'$. Let $\Delta = \{\alpha : \Box_A \alpha \in \Gamma\}$. By construction, $\Gamma' \supseteq \Delta$ Assume, for a contradiction, that $\Box_A \phi \notin \Gamma$. By the saturation condition (2), $\Gamma \nvdash \Box_A \phi$. Then, by Lemma 4.5, $\Delta \nvdash \phi$. By Lemma 4.4, there is a saturated extension Δ^* such that $\Delta^* \nvdash \phi$. This contradicts the fact that, for all Γ' such that $\Gamma R_A \Gamma'$, $\phi \in \Gamma'$, i.e., that (by construction of the canonical model), for all saturated sets Γ' such that $\Gamma' \supseteq \Delta$, $\phi \in \Gamma'$. The converse is trivial.

■

To show that the canonical model $\mathbf{M}$ defined above is indeed a model, we have to prove that it satisfies conditions (a)-(d).

Lemma 4.8 *Let* $\mathbf{M}$ *be the canonical model as defined in Definition 4.6.* $\mathbf{M}$ *satisfies the semantic conditions (a), (b), (c), and (d).*

Proof. We have to prove that

(a) $\forall \Gamma, \Gamma', \Gamma'' \in S$, if $\Gamma \leq \Gamma'$ and $\Gamma' R_A \Gamma''$ then $\Gamma R_A \Gamma''$

(b) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$ then $\Gamma \leq \Gamma'$.

(c) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$ then $\Gamma' R_A \Gamma'$.

(d) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$ and $\vdash A \leftrightarrow B$ then $\Gamma R_B \Gamma'$.

The proof is straightforward. As an example, let us prove point (b). Given a saturated set Γ, we have to show that if $\Gamma R_A \Gamma'$ then $\Gamma \leq \Gamma'$. Assume that $\Gamma R_A \Gamma'$ and let $\alpha \in \Gamma$. By saturation of Γ and by (UNIT), $\alpha \rightarrow \Box_A \alpha \in \Gamma$. By (MP), $\Box_A \alpha \in \Gamma$. Hence, by construction of the canonical model, $\alpha \in \Gamma'$. Therefore, $\Gamma \leq \Gamma'$.

■

By the above lemmas, we can conclude that:

Theorem 4.9 (Completeness) *The axiomatization of the logic* CC_{AC} *given in Section 2 is complete with respect to the Kripke semantics in Section 3, that is: given a formula* $A \in \mathcal{L}$*, if* $\Gamma \models A$*, then* $\Gamma \vdash A$

Proof. For a contradiction, suppose $\Gamma \nvdash A$. Then by lemma 4.4 there is a saturated extension Γ^* of Γ such that $\Gamma^* \nvdash A$. By Definition 4.6 and lemmas 4.7 4.8, we conclude that there is a (canonical) model $M = (S, \leq, \{R_A\}, \Gamma^*, h)$ such that $M, \Gamma^* \models \Gamma^*$ and $M, \Gamma^* \not\models A$, hence $\Gamma^* \not\models A$. Since $\Gamma \subseteq \Gamma^*$, also $M, \Gamma^* \models \Gamma$, hence $\Gamma \not\models A$. ■

5 Conclusions

We have defined an intuitionistic conditional logic for Access Control (CC_{AC}) by providing an axiomatization and a Kripke model semantics. We have proven that the axiomatization is sound and complete with respect to the semantics. In CC_{AC}, principals are defined as arbitrary formulas. The generality of the language makes it possible to formalize, for instance, the so called boolean principals [2], that is, principals which are formed by boolean combinations of atomic principals. For the time being, CC_{AC} only includes few uncontroversial axioms of access control logics but it can be extended in order to cope with richer axioms. This is what we plan to do in future work.

References

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

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

[3] A.S. Troelstra and D. van Dalen, *Constructivism in Mathematics: An Introduction*, North-Holland Publishing, Amsterdam.