A constructive conditional logic for access control: a preliminary report

Valerio Genovese‡ and Laura Giordano* and Valentina Gliozzi♣ and Gian Luca Pozzato♠

Abstract. We define an Intuitionistic Conditional Logic for Access Control called $C_{ICL}$. The logic $C_{ICL}$ is based on a conditional language allowing principals to be defined as arbitrary formulas and it includes few uncontroversial axioms of access control logics. We provide an axiomatization and a Kripke model semantics for the logic $C_{ICL}$, and we prove that the axiomatization is sound and complete with respect to the semantics.

1 Introduction

Access control is concerned with the decision of accepting or denying 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 [2, 3, 10, 11, 12].

A common feature of most well-known approaches is the employment of constructive logics enriched with formulas of the form $A \text{ says } \varphi$, intuitively meaning that the principal $A$ asserts or supports $\varphi$ to hold in the system. In [1] it is shown that an intuitionistic interpretation of the modality "says" allows to avoid unexpected conclusions that are derivable when "says" is given an axiomatization in classical logic.

The treatment of the operator "says" as a modality can be found in [4], which introduces a logical framework, FSL, based on modal logic methodology. In [6] an access control logic, ICL, is defined as an extension of intuitionistic propositional logic, in which the operator "says" is given a modal interpretation in the logic S4.

In this paper we show that conditional logics [13] can provide a natural framework to define axiomatization and semantics for access control logics. We present an intuitionistic logic, $C_{ICL}$, which integrates access control logics with conditional logics. We formalize the says operator as a conditional normal modality so that $A \text{ says } \phi$ is regarded as a conditional implication $A \Rightarrow \phi$, meaning that proposition $\phi$ holds in all the preferred worlds for the principal $A$. The generality of this approach opens the way to the formalization of the so-called boolean principals [6], that is, principals which are formed by boolean combination of atomic principals.

From the access control point of view, the says operator satisfies the axioms of the “basic logic of access control” ICL [6].

2 The logic $C_{ICL}$

We introduce the conditional intuitionistic logic $C_{ICL}$ for access control by defining its axiomatization and Kripke semantics. The formulation of the says modality as a conditional operator allows boolean principals to be modelled in a natural way, since in a conditional formula $A \text{ says } \phi$, both $A$ and $\phi$ are arbitrary formulas. For instance, we can write, $A \land B \text{ says } \phi$ to mean that principals $A$ and $B$ jointly say that $\phi$, and $A \lor B \text{ says } \phi$ to mean that principals $A$ and $B$ independently say that $\phi$. Indeed, conditional logics provide a natural generalization of multimodal logics to the case when modalities are labelled by arbitrary formulas.

We define the language $L$ of the logic $C_{ICL}$. Let $ATM$ be a set of atomic propositions. The formulas of $L$ are defined inductively as follows: if $P \in ATM$, then $P \in L$; $\bot \in L$, where $\bot$ is a proposition which is always false; if $A, \varphi, \varphi_1$ and $\varphi_2$ are formulas of $L$, then $\neg \varphi, \varphi_1 \land \varphi_2, \varphi_1 \lor \varphi_2, \varphi_1 \rightarrow \varphi_2$, and $A \text{ says } \varphi$ are formulas of $L$.

The intended meaning of the formula $A \text{ says } \psi$, where $A$ and $\psi$ are arbitrary formulas, is that principal $A$ says that $\psi$, namely, "the principal $A$ asserts or supports $\psi"$ [6]. Although the principal $A$ 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.

The axiom system of the logic $C_{ICL}$ contains the following axioms and inference rules:

- (TAUT) all tautologies of intuitionistic logic
- (K) $A \text{ says } (\alpha \rightarrow \beta) \rightarrow (A \text{ says } \alpha \rightarrow A \text{ says } \beta)$
- (UNIT) $\alpha \rightarrow (A \text{ says } \alpha)$
- (C4) $(A \text{ says } (A \text{ says } \alpha)) \rightarrow (A \text{ says } \alpha)$
- (MP) If $\vdash \alpha$ and $\vdash \alpha \rightarrow \beta$ then $\vdash \beta$
- (RCEA) If $\vdash A \rightarrow \beta$ then $\vdash (A \text{ says } \gamma) \rightarrow (B \text{ says } \gamma)$
- (RCK) If $\vdash \alpha \rightarrow \beta$ then $\vdash (A \text{ says } \alpha) \rightarrow (A \text{ says } \beta)$

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 $\vdash \phi$ then $\vdash \Box \phi$) in modal/multimodal logic. The axiom (K) belongs to the axiomatization of all normal modal logics and it is derivable in “normal” conditional logics. (UNIT), (K) and (C4) are the characterizing axioms of the access control logics ICL [6]. All the tautologies of intuitionistic logic are included, so that the resulting logic is an intuitionistic version of a conditional logic. As a major difference with ICL axiomatization [6], our axiomatization above also includes the inference rule (RCEA) for the says modality, which allows to deal with equivalent principals.

The semantics of the logic $C_{ICL}$ is a standard Kripke semantics and is defined as follows:

Definition 1 A $C_{ICL}$ model has the form $M = (S, \preceq, \{ R_A \}, t_0, h)$ where: $S \neq \emptyset$ is a set of items called worlds; $\preceq$ is a partial order

1. University of Luxembourg and Università di Torino, Italy, email: valerio.genovese@uni.lu - • Dip. di Informatica, Università del Piemonte Orientale, Alessandria, Italy, email: laura@mf.unipmn.it - ♣ Dip. di Informatica, Università degli Studi di Torino, Italy, email: gliozzi.pozzato@di.unito.it. The work has been partially supported by Regione Piemonte, Project “ICT4Law”. Valerio Genovese is supported by the National Research Fund, Luxembourg.
over \( S \); \( R_A \) is a binary relation on \( S \) associated with the formula \( A \); \( t_0 \in S \); \( \text{h is an evaluation function ATM} \rightarrow \text{Pow}(S) \) 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 \( M, t \models \phi \), as follows. We use \([\phi]_t\) to denote \( \{ y \in S \mid M, y \models \phi \} \).

1. \( M, t \models \varphi \wedge \psi \) iff \( M, t \models \varphi \) and \( M, t \models \psi \).
2. \( M, t \models \varphi \vee \psi \) iff \( M, t \models \varphi \) or \( M, t \models \psi \).
3. \( M, t \models \varphi \rightarrow \psi \) iff for all \( s \) such that \( t \leq s \) (if \( M, s \models \varphi \) then \( M, s \models \psi \)).
4. \( M, t \models \neg \varphi \) iff for all \( s \) such that \( t \leq s \), \( M, s \not\models \varphi \).
5. \( M, t \not\models \bot \).
6. \( M, t \models \top \).

We say that \( \phi \) is valid in a model \( M \) if \( M, t_0 \models \phi \). We say that \( \phi \) is true at \( t \) (and \( \models \phi \) if \( \phi \) is valid in every model. We extend the notion of validity to a set of formulas \( \Gamma \) in the obvious way: \( M, t_0 \models \Gamma \) iff \( M, t_0 \models \psi \) for all \( \psi \in \Gamma \). Last, we say that \( \phi \) is a logical consequence of \( \Gamma \) (and \( \Gamma \models \psi \) if, for all models \( M \), \( M, t_0 \models \Gamma \), then \( M, t_0 \models \psi \)).

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

(a) \( \forall t, s, z \in S, s \leq t \) and \( t R_A z \) then \( z R_A s \);
(b) \( \forall t, s \in S, s \neq s R_A t \) then \( s \leq t \);
(c) \( \forall t, s \in S, s R_A t \) then \( \exists s, z \in S \text{ such that } s R_A z \) and \( z R_A t \);
(d) if \( \| [A] \| = \| [B] \| \), then \( R_A = R_B \).

Conditions (b) and (c) are, respectively, the semantic conditions associated with the axioms (UNIT) and (C4), while condition (a) is needed to enforce the property that a formula true in a world \( s \) is also true in all worlds reachable from \( s \) by the relation \( \leq \) (i.e., in all worlds \( t \) such that \( s \leq t \)). Condition (d) is the well-known condition for normality in conditional logics, 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 formulations of conditional logic semantics. In particular, \( s R_A t \) corresponds to \( t \in f(A, s) \), and conditions (a), (b), (c) and (d) above are indeed conditions on the selection function \( f \), as usual in conditional logics.

It is worth noticing that the notion of logical consequence defined above can be used to verify that a request \( \varphi \) of a principal \( A \) is compliant with a set of policies. Intuitively, given a set of formulas \( \Gamma \) representing policies, we say that \( A \) is compliant with \( \Gamma \) iff \( \Gamma \text{ says } \varphi \Rightarrow \varphi \). For instance, if \( \Gamma = \{(\text{admin says delete file1}) \rightarrow \text{delete file1}\} \), then \( \Gamma \text{ says } \text{Bob says delete file1} \Rightarrow \text{delete file1} \).

The axiomatization of the logic \( C_{\text{ICL}} \) outlined above is sound and complete w.r.t. the semantics in Definition 1 (see [9] for the proof):

**Theorem 1** Given a formula \( \varphi \in L \), \( \varphi \) if and only if \( \models \varphi \).

**3 Conclusions**

We have defined an intuitionistic conditional logic for Access Control (\( C_{\text{ICL}} \)) by providing an axiomatization and a Kripke model semantics. An analytic, cut-free, labelled sequent calculus for the logic \( C_{\text{ICL}} \) has been provided in [9]. In \( C_{\text{ICL}} \), principals are defined as arbitrary formulas. The generality of the language makes it possible to formalize, for instance, the so-called boolean principals [6], that is, principals which are formed by boolean combinations of atomic principals. For the time being, \( C_{\text{ICL}} \) only includes few uncontroversial axioms of access control logics but it can be extended in order to cope with richer axioms. A discussion of the properties of boolean principals can be found in [9].

From an axiomatic point of view, the employment of constructive logics for access control has been put forward by Abadi in [1], where he shows that from (UNIT) axiom in classical logic we can deduce \( A \text{ says } \varphi \rightarrow (\varphi \vee A \text{ says } \psi) \). The previous axioms is called (Escalation) and it represents a rather degenerate interpretation of says, i.e., if \( A \text{ says } \varphi \), either \( \varphi \) is permitted or the principal can say anything. On the contrary, if we interpret the says within an intuitionistic logic we can avoid (Escalation). More generally, as put forward in [8, 14], 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 instance, we can prove \( \psi \) using a classical logic by proving \( \varphi \rightarrow \psi \) and \( \neg \varphi \rightarrow \psi \), since from these theorems we can conclude \( (\varphi \vee \neg \varphi) \rightarrow \psi \), hence \( T \rightarrow \psi \).

From a logical point of view, several formal systems have been developed in the recent years [2, 3, 7, 10, 11, 12]. Up to authors knowledge, the only works that introduce a logic for access control with a Kripke semantics, a calculus and a completeness result are [5, 6]. In [5], principals are atomic and they cannot be combined, moreover the underlying semantics is constructive S4 enriched with views, i.e. a mapping from worlds to sets of principals, this approach breaks the useful bound between axioms of says and accessibility relationships and, as a consequence, [5] does not provide canonical properties for its axioms. In [6] the authors provide an axiomatization of ICL, a sequent calculus for it and a translation of ICL into modal logic S4. They also present extensions of ICL for dealing with delegation (ICL\text{\textsuperscript{De}}) and with boolean principals (ICL\text{\textsuperscript{B}}).

**REFERENCES**