A constructive conditional logic for access control: a preliminary report

Valerio Genovese$^{\diamondsuit}$ and **Laura Giordano**$^{\bullet}$ and **Valentina Gliozzi**$^{\clubsuit}$ and **Gian Luca Pozzato**$^{\clubsuit}$[1]

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 **says** φ, intuitively meaning that the principal A *asserts* or *supports* φ 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 multimodal 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 **says** ϕ is regarded as a conditional implication $A \Rightarrow \phi$, meaning that proposition ϕ 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].

[1] $^{\diamondsuit}$ University of Luxembourg and Università di Torino, Italy, email: valerio.genovese@uni.lu - $^{\bullet}$ Dip. di Informatica, Università del Piemonte Orientale, Alessandria, Italy, email: laura@mfn.unipmn.it - $^{\clubsuit}$ 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.

2 The logic $C_{\mathbf{ICL}}$

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 **says** ϕ, both A and ϕ are arbitrary formulas. For instance, we can write, $A \wedge B$ **says** ϕ to mean that principals A and B jointly say that ϕ, and $A \vee B$ **says** ϕ to mean that principals A and B independently say that ϕ. Indeed, conditional logics provide a natural generalization of multimodal logics to the case when modalities are labelled by arbitrary formulas.

We define the language $\mathcal{L}$ of the logic C_{ICL} . Let ATM be a set of atomic propositions. The formulas of $\mathcal{L}$ are defined inductively as follows: if $P \in ATM$, then $P \in \mathcal{L}$; $\bot \in \mathcal{L}$, where $\bot$ is a proposition which is always false; if A, φ, φ_1 and φ_2 are formulas of $\mathcal{L}$, then $\neg\varphi$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\varphi_1 \rightarrow \varphi_2$, and A **says** φ are formulas of $\mathcal{L}$.

The intended meaning of the formula A **says** ψ, where A and ψ are arbitrary formulas, is that *principal* A *says that* ψ, namely, "the principal A asserts or supports ψ" [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 **says** $(\alpha \rightarrow \beta) \rightarrow (A$ **says** $\alpha \rightarrow A$ **says** $\beta)$
(UNIT)	$\alpha \rightarrow (A$ **says** $\alpha)$
(C4)	$(A$ **says** $(A$ **says** $\alpha)) \rightarrow (A$ **says** $\alpha)$
(MP)	If $\vdash \alpha$ and $\vdash \alpha \rightarrow \beta$ then $\vdash \beta$
(RCEA)	If $\vdash A \leftrightarrow B$ then $\vdash (A$ **says** $\gamma) \leftrightarrow (B$ **says** $\gamma)$
(RCK)	If $\vdash \alpha \rightarrow \beta$ then $\vdash (A$ **says** $\alpha) \rightarrow (A$ **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 taultologies 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 $\mathcal{M} = (S, \leq, \{R_A\}, t_0, h)$ 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 $\mathcal{M}$, by the relation $\mathcal{M}, t \models \phi$, as follows. We use $[|\phi|]$ to denote $\{y \in S \mid \mathcal{M}, y \models \phi\}$.

1. *$\mathcal{M}, t \models P \in ATM$ iff, for all s such that $t \leq s$, $s \in h(P)$*
2. *$\mathcal{M}, t \models \varphi \wedge \psi$ iff $\mathcal{M}, t \models \varphi$ and $\mathcal{M}, t \models \psi$*
3. *$\mathcal{M}, t \models \varphi \vee \psi$ iff $\mathcal{M}, t \models \varphi$ or $\mathcal{M}, t \models \psi$*
4. *$\mathcal{M}, t \models \varphi \rightarrow \psi$ iff for all s such that $t \leq s$ (if $\mathcal{M}, s \models \varphi$ then $\mathcal{M}, s \models \psi$)*
5. *$\mathcal{M}, t \models \neg\varphi$ iff, for all s such that $t \leq s$, $\mathcal{M}, s \not\models \varphi$*
6. *$\mathcal{M}, t \not\models \bot$*
7. *$\mathcal{M}, t \models A$ **says** ψ iff, for all s such that tR_As, $\mathcal{M}, s \vDash \psi$.*

We say that ϕ is valid in a model $\mathcal{M}$ if $\mathcal{M}, t_0 \models \phi$. 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: $\mathcal{M}, t_0 \models \Gamma$ if $\mathcal{M}, t_0 \models \psi$ 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 $\mathcal{M}$, if $\mathcal{M}, t_0 \models \Gamma$, then $\mathcal{M}, t_0 \models \phi$.*

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 $s \leq t$;
(c) $\forall t, s \in S$, if sR_At, then $\exists z \in S$ such that sR_Az and zR_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 (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, sR_At 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 φ of a principal A is compliant with a set of policies. Intuitively, given a set of formulas Γ representing policies, we say that A is compliant with Γ iff Γ, A **says** $\varphi \models \varphi$. For instance, if $\Gamma = \{((admin$ **says** $deletefile1) \rightarrow deletefile1), admin$ **says** $(Bob$ **says** $deletefile1 \rightarrow deletefile1)\}$, we obtain that Γ, Bob **says** $deletefile1 \models deletefile1$.

The axiomatization of the logic C_{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 $\varphi \in \mathcal{L}$, $\vdash \varphi$ if and only if $\models \varphi$.*

3 Conclusions

We have defined an intuitionistic conditional logic for Access Control (C_{ICL}) by providing an axiomatization and a Kripke model semantics. An analytic, cut-free, labelled sequent calculus for the logic C_{ICL} has been provided in [9]. In C_{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_{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 **says** $\varphi \rightarrow (\varphi \vee A$ **says** $\psi)$. The previous axioms is called (Escalation) and it represtents a rather degenerate interpretation of says, i.e., if A says φ, either φ 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 ψ 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 $\top \rightarrow \psi$.

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$^{\Rightarrow}$) and with boolean principals (ICL$^{\mathcal{B}}$).

REFERENCES

[1] M. Abadi, 'Variations in access control logic', in *DEON08*, pp. 96–109.
[2] M. Abadi, M. Burrows, B. W. Lampson, and G. D. Plotkin, 'A calculus for access control in distributed systems', in *CRYPTO 91*, pp. 1–23.
[3] C. Bertolissi, M. Fernández, and S. Barker, 'Dynamic event-based access control as term rewriting', in *DBSec07*, pp. 195–210.
[4] G. Boella, D. Gabbay, V. Genovese, and L. van der Torre, 'Fibred security language', *Studia Logica*, **92**(3), 395–436, (2009).
[5] D. Garg, 'Principal centric reasoning in constructive authorization logic', in *Informal Proc. of IMLA*, (2008).
[6] D. Garg and M. Abadi, 'A modal deconstruction of access control logics', in *FoSSaCS 08*, pp. 216–230, Budapest, Hungary.
[7] D. Garg, L. Bauer, K. Bowers, F. Pfenning, and M. Reiter, 'A linear logic of authorization and knowledge', in *ESORICS 06*, pp. 297–312.
[8] Deepak Garg and Frank Pfenning, 'Non-interference in constructive authorization logic', in *CSFW-19*, pp. 283–296, (2006).
[9] V. Genovese, L. Giordano, V. Gliozzi, and G. L. Pozzato, 'A Constructive Conditional Logic for Access Control: a completeness result and a sequent calculus', *Proc. of CILC2010, also available as Technical Report 127/2010 of Dip. di Informatica, Univ. di Torino, http://www.di.unito.it/~argo/papers/TR1272010.pdf*.
[10] Y. Gurevich and A. Roy, 'Operational semantics for DKAL: Application and analysis', in *TrustBus 2009*, pp. 149–158.
[11] C. Lesniewski-Laas, B. Ford, J. Strauss, R. Morris, and M. F. Kaashoek, 'Alpaca: extensible authorization for distributed services', in *Proc. of ACM CCS 2007*, pp. 432–444.
[12] N. Li, B. N. Grosof, and J. Feigenbaum, 'Delegation logic: A logic-based approach to distributed authorization', *ACM Trans. Inf. Syst. Secur.*, **6**(1), 128–171, (2003).
[13] D. Nute, *Topics in Conditional Logic*, Reidel, Dordrecht, 1980.
[14] E. Sire, F. Schneider, and K. Walsh, 'Nexus authorization logic (nal): Design rationale and applications', Technical report, (2009).