Access Control Policy Differentiation through Narrowing

Clara Bertolissi, Jean-Marc Talbot and Didier Villevalois
LIF, Aix-Marseille University & CNRS, France

Differentiation Problem

Problem:
Differentiation of two access control policies by enumerating counter-examples to equivalence

Motivation:
Assistance in the maintenance of access control policies

Access Control Policies [1, 2]

Access control policies specify when a request for an action by a user on a resource can be granted or not.

Access control policies can be formally specified as **term rewrite systems**. Requests can be encoded as ground terms and thus be evaluated through rewriting.

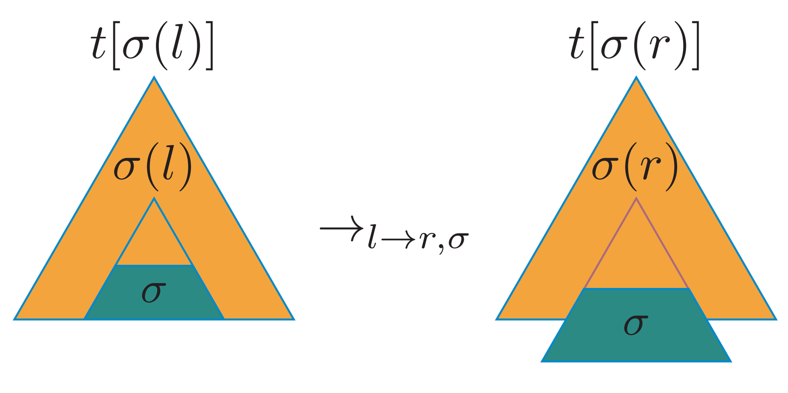
Also one can **verify semi-automatically some properties** of the policy by verifying the equivalent properties on the corresponding term rewrite system:

— Consistence ⇝ Confluence
— Completeness ⇝ Totality
— Termination ⇝ Termination

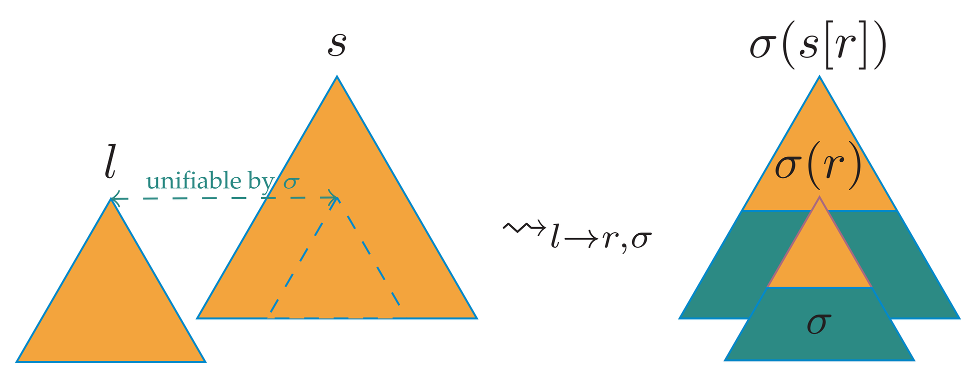
Rewriting vs. Narrowing [3]

Narrowing is a generalization of rewriting. Input terms can contain variables that will be bound in the process of narrowing.

Rewriting matches instances of rule left-hand sides:



Narrowing unifies sub-terms with rule left-hand sides:



Thus narrowing can be used for **equation resolution**:

$$t_1 \approx t_2 \overset{*}{\rightsquigarrow}_{\mathcal{R},\sigma} \mathsf{true} \implies \sigma \text{ is a } \mathcal{R}\text{-unifier of } t_1 \text{ and } t_2$$
(i.e. σ is a solution to the equation $t_1 \approx t_2$ in $\mathcal{R}$)

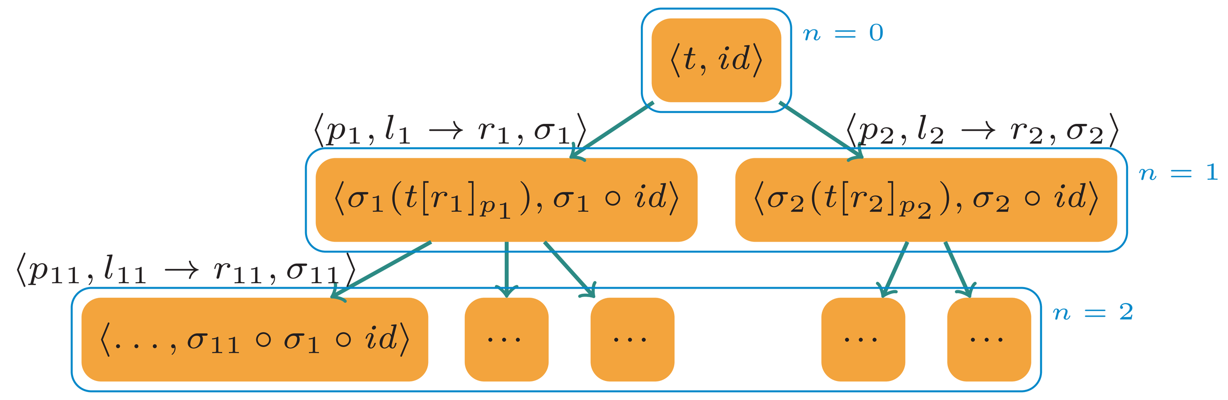
An administrator might use narrowing to answer more complex queries about a policy.

We use this technique to compute the differential between two versions of a policy for some query term.

Breadth-First Search of Narrowings

The derivations of t of length $n \in \mathbb{N}$ by a strategy $\mathcal{S}$:

$$\mathcal{N}^n_{\mathcal{S}}(t) \ni \begin{cases} \langle t, id\rangle & \text{si } n = 0 \\ \langle \sigma(s[r]_p), \sigma \circ \tau\rangle & \text{si } n > 0 \\ & \text{and } \langle s, \tau\rangle \in \mathcal{N}^{n-1}_{\mathcal{S}}(t) \\ & \text{and } \langle p, l \to r, \sigma\rangle \in \mathcal{S}(s) \end{cases}$$

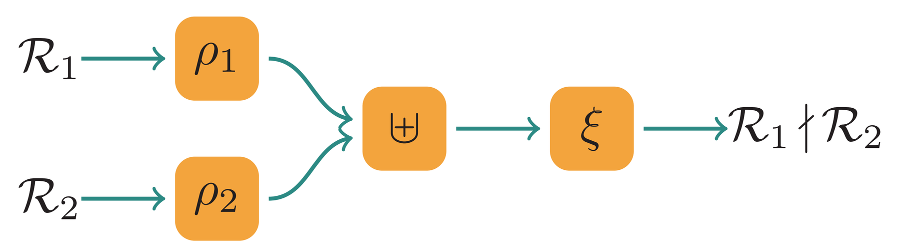


On a Common Set of Constructors ($\mathcal{C} = \mathcal{C}_1 = \mathcal{C}_2$)

Definition 1. Let $\mathcal{C}$ be a set of constructors, $\mathcal{D}_1$ and $\mathcal{D}_2$ two sets of operations such that $\mathcal{D}_1 \cap \mathcal{D}_2 \neq \emptyset$, $\mathcal{F}_1 = (\mathcal{C} \uplus \mathcal{D}_1)$ and $\mathcal{F}_2 = (\mathcal{C} \uplus \mathcal{D}_2)$ two signatures, and $\mathcal{R}_1 = (\mathcal{F}_1, R_1)$ and $\mathcal{R}_2 = (\mathcal{F}_2, R_2)$ two inductively sequential rewrite systems. Let $t \in \mathcal{T}(\mathcal{F}_1 \cap \mathcal{F}_2, \mathcal{X})$ be an operation-rooted term. Then the **narrowing differential of t in $\mathcal{R}_2$ w.r.t. $\mathcal{R}_1$** is

$$\mathbf{D}_{\mathcal{R}_1,\mathcal{R}_2}(t) \overset{\text{def}}{=} \{(\sigma, v_1, v_2) \in (\mathcal{V}(t) \to \mathcal{T}(\mathcal{C}, \mathcal{X})) \times \mathcal{T}(\mathcal{C}) \times \mathcal{T}(\mathcal{C}) \mid \sigma(t) \overset{*}{\to}_{\mathcal{R}_1} v_1 \text{ and } \sigma(t) \overset{*}{\to}_{\mathcal{R}_2} v_2 \text{ and } v_1 \neq v_2\}$$

We build a new system $\mathcal{R}_1 \nmid \mathcal{R}_2$ from $\mathcal{R}_1$ and $\mathcal{R}_2$.



where ρ_k renames operations o to o_k in every rules, and ξ extends with rules for the $\wedge$, $\approx$ and $\not\approx$ operations.

We build $\hat{t} \overset{\text{def}}{=} (\rho_1(t) \approx x \wedge \rho_2(t) \approx y \wedge x \not\approx y)$, with x, y two fresh variables, that **we narrow in** $\mathcal{R}_1 \nmid \mathcal{R}_2$.

Theorem 1 (Soundness).
$$\hat{t} \overset{*}{\rightsquigarrow}_{\mathcal{R}_1 \nmid \mathcal{R}_2, \sigma} \mathsf{true} \implies (\sigma_{|\mathcal{V}(t)}, \sigma(x), \sigma(y)) \in \mathbf{D}_{\mathcal{R}_1,\mathcal{R}_2}(t)$$

Theorem 2 (Completeness).
$$(\sigma, v_1, v_2) \in \mathbf{D}_{\mathcal{R}_1,\mathcal{R}_2}(t) \implies \hat{t} \overset{*}{\rightsquigarrow}_{\mathcal{R}_1 \nmid \mathcal{R}_2, \sigma'} \mathsf{true}$$
where $\sigma' = \sigma \cup \{x \mapsto v_1, y \mapsto v_2\}[\mathcal{V}(t) \cup \{x, y\}]$

On Non-disjoint Sets of Constructors ($\mathcal{C}_1 \cap \mathcal{C}_2 \neq \emptyset$)

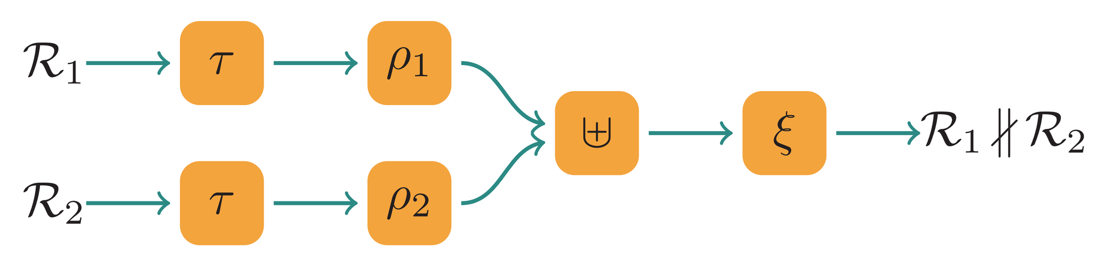
Definition 2. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two sets of constructors such that $\mathcal{C}_1 \cap \mathcal{C}_2 \neq \emptyset$, $\mathcal{D}_1$ and $\mathcal{D}_2$ two sets of operations such that $\mathcal{D}_1 \cap \mathcal{D}_2 \neq \emptyset$, $\mathcal{F}_1 = (\mathcal{C}_1 \uplus \mathcal{D}_1)$ and $\mathcal{F}_2 = (\mathcal{C}_2 \uplus \mathcal{D}_2)$ two signatures, and $\mathcal{R}_1 = (\mathcal{F}_1, R_1)$ and $\mathcal{R}_2 = (\mathcal{F}_2, R_2)$ two inductively sequential rewrite systems. Let $t \in \mathcal{T}(\mathcal{F}_1 \cap \mathcal{F}_2, \mathcal{X})$ be an operation-rooted term. We define

$$\mathbf{D}^{-}_{\mathcal{R}_1,\mathcal{R}_2}(t) \overset{\text{def}}{=} \{(\sigma, v_1, \bot) \in (\mathcal{V}(t) \to \mathcal{T}(\mathcal{C}_1, \mathcal{X})) \times \mathcal{T}(\mathcal{C}_1) \times \{\bot\} \mid \sigma(t) \overset{*}{\to}_{\mathcal{R}_1} v_1 \text{ and } \sigma(t) \notin \mathcal{T}(\mathcal{C}_2 \uplus \mathcal{D}_2, \mathcal{X})\}$$
$$\mathbf{D}^{+}_{\mathcal{R}_1,\mathcal{R}_2}(t) \overset{\text{def}}{=} \{(\sigma, \bot, v_2) \in (\mathcal{V}(t) \to \mathcal{T}(\mathcal{C}_2, \mathcal{X})) \times \{\bot\} \times \mathcal{T}(\mathcal{C}_2) \mid \sigma(t) \overset{*}{\to}_{\mathcal{R}_2} v_2 \text{ and } \sigma(t) \notin \mathcal{T}(\mathcal{C}_1 \uplus \mathcal{D}_1, \mathcal{X})\}$$
$$\mathbf{D}^{\neq}_{\mathcal{R}_1,\mathcal{R}_2}(t) \overset{\text{def}}{=} \{(\sigma, v_1, v_2) \in (\mathcal{V}(t) \to \mathcal{T}(\mathcal{C}_1 \cap \mathcal{C}_2, \mathcal{X})) \times \mathcal{T}(\mathcal{C}_1) \times \mathcal{T}(\mathcal{C}_2) \mid \sigma(t) \overset{*}{\to}_{\mathcal{R}_1} v_1 \text{ and } \sigma(t) \overset{*}{\to}_{\mathcal{R}_2} v_2 \text{ and } v_1 \neq v_2\}$$

Then the **narrowing differential of t in $\mathcal{R}_2$ w.r.t. $\mathcal{R}_1$** is

$$\mathbf{D}^{\pm}_{\mathcal{R}_1,\mathcal{R}_2}(t) \subseteq (\mathcal{V}(t) \to \mathcal{T}(\mathcal{C}_1 \cup \mathcal{C}_2, \mathcal{X})) \times (\mathcal{T}(\mathcal{C}_1) \cup \bot) \times (\mathcal{T}(\mathcal{C}_2) \cup \bot)$$
$$\mathbf{D}^{\pm}_{\mathcal{R}_1,\mathcal{R}_2}(t) \overset{\text{def}}{=} \mathbf{D}^{-}_{\mathcal{R}_1,\mathcal{R}_2}(t) \cup \mathbf{D}^{\neq}_{\mathcal{R}_1,\mathcal{R}_2}(t) \cup \mathbf{D}^{+}_{\mathcal{R}_1,\mathcal{R}_2}(t)$$

We build a new system $\mathcal{R}_1 \nparallel \mathcal{R}_2$ from $\mathcal{R}_1$ and $\mathcal{R}_2$.



Where $\tau(\mathcal{R}_k)$ rewrites as $\mathcal{R}_k$ on $\mathcal{C}_k$ and to $\bot$ otherwise.

We build $\hat{t} \overset{\text{def}}{=} (\rho_1(t) \approx x \wedge \rho_2(t) \approx y \wedge x \not\approx y)$, with x, y two fresh variables, that **we narrow in** $\mathcal{R}_1 \nparallel \mathcal{R}_2$.

Theorem 3 (Soundness).
$$\hat{t} \overset{*}{\rightsquigarrow}_{\mathcal{R}_1 \nparallel \mathcal{R}_2, \sigma} \mathsf{true} \implies (\sigma_{|\mathcal{V}(t)}, \sigma(x), \sigma(y)) \in \mathbf{D}^{\pm}_{\mathcal{R}_1,\mathcal{R}_2}(t)$$

Theorem 4 (Completeness).
$$(\sigma, v_1, v_2) \in \mathbf{D}^{\pm}_{\mathcal{R}_1,\mathcal{R}_2}(t) \implies \hat{t} \overset{*}{\rightsquigarrow}_{\mathcal{R}_1 \nparallel \mathcal{R}_2, \sigma'} \mathsf{true}$$
where $\sigma' = \sigma \cup \{x \mapsto v_1, y \mapsto v_2\}[\mathcal{V}(t) \cup \{x, y\}]$

Results

The **differential of two access control policies** for some query term is **recursively enumerable**.

Indeed, both $\mathbf{D}_{\mathcal{R}_1,\mathcal{R}_2}(t)$ and $\mathbf{D}^{\pm}_{\mathcal{R}_1,\mathcal{R}_2}(t)$ are recursively enumerable, by narrowing $\hat{t}$ in $\mathcal{R}_1 \nmid \mathcal{R}_2$ and $\mathcal{R}_1 \nparallel \mathcal{R}_2$ in a breadth-first search manner, even though the number of solutions can be unbounded, or $\mathcal{R}_1$ and/or $\mathcal{R}_2$ non-terminating.

Inductive Sequentiality [4, 5]

Constructor-Based Rewrite Systems:
Functions are partitioned in *constructors* and *defined operations*; Rewrite rules eliminate defined operations.

Inductively Sequential Rewrite Systems:
Constructor-based rewrite systems that are orthogonal by construction.

Outermost Needed Narrowing:
A narrowing strategy that makes use of inductive sequentiality to always apply rules at the outermost position that will be narrowed in any derivation.

$$\mathcal{S} : t \mapsto \{\langle p, l \to r, \sigma\rangle \mid t \rightsquigarrow_{p, l\to r, \sigma} \sigma(t[r]_p)\}$$

In this work, we restrict to inductively sequential rewrite systems and the outermost needed narrowing.

References

[1] S. Barker. The next 700 access control models or a unifying meta-model? In *SACMAT 2009, 14th ACM Symposium on Access Control Models and Technologies, Stresa, Italy, June 3-5, 2009, Proceedings*, pages 187–196, 2009.

[2] C. Bertolissi and M. Fernández. Category-Based Authorisation Models: Operational Semantics and Expressive Power. pages 140–156, 2010. 00002.

[3] A. Middeldorp and E. Hamoen. Completeness Results for Basic Narrowing. *Applicable Algebra in Engineering, Communication and Computing*, 5(3-4):213–253, 1994. 00138.

[4] S. Antoy. Definitional Trees. In *In Proc. of the 3rd International Conference on Algebraic and Logic Programming*, pages 143–157. Springer LNCS, 1992.

[5] S. Antoy, R. Echahed, and M. Hanus. A Needed Narrowing Strategy. In *Proceedings of the 21st ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 268–279. ACM, 1994. 00415.

Contact Information

http://pageperso.lif.univ-mrs.fr/~didier.villevalois/
didier.villevalois@lif.univ-mrs.fr
+33 (0)4 91 82 95 25
LIF, TPR1, Bureau 545, Luminy, Marseille