Permission to Speak: An Access Control Logic

Nikhil Dinesh  Aravind Joshi  Insup Lee  Oleg Sokolsky

Department of Computer and Information Science
University of Pennsylvania

FLACOS 2008
November 27-28, 2008
Outline

1. Introduction and motivation
2. System Architecture
3. Inference component
4. Policies and conformance
5. Examples
Goal: analysis of regulated operations
- Bloodbanks (in the US, subject to FDA regulations)
- Medical records (in the US, subject to HIPAA)

Regulatory documents
- Natural language
  - Explicit references to connect sentences
  - Lots of exceptions
- Translate to logic one sentence at a time
  - Provide traceability
  - Reduce complexity

This talk: access control
The problem of access control:

- Should a request be granted?

I want to print this... My manager says I can

I am not required to listen to your manager

Questions to answer:

- which policies need to be consulted in granting access?
- which policies are violated and who is to blame?
Access control vs. conformance

Policy-based regulation

- A policy specifies what actions are permitted to happen and what are required to happen
- A policy is issued by an authority
  - A large system may have multiple sources of authority
- Possible actions include
  - Performing access
  - Delegating or authorizing access
  - Delegating the right to authorize access

- Access control is a special case of conformance checking
Deontic policies

Need a framework to combine
- Permission and obligation: deontic modalities
- “Saying”: policy/credential introduction

Challenges
- Representation and authorization
- Positive and negative permissions
- Nested deontic modalities
# Representation in access control

## The saying modality

A says $\varphi$ in the laws $l(A)$: $\text{says}_{l(A)}\varphi$

## Representation

- $B$ speaks using the authority of $A$
  - Allows us to handle authorization and delegation
  - $B$ should be able to make only authorized statements
    - Clear interplay with the notion of permission
- Many formalizations in access control literature
  - Hand-off axiom
  - Many pitfalls to avoid
  - No explicit representation of permissions
Representation: our approach

**Axiom of representation**

If $A$ says that $B$ is allowed to say $\varphi$, then if $B$ says $\varphi$, $A$ says $\varphi$

$$\text{says}_{l(A)}(\mathcal{P}_B \text{says}_{l(B)} \varphi) \land \text{says}_{l(B)} \varphi \Rightarrow \text{says}_{l(A)} \varphi$$

**Advantages**

- Decidable logic with complete semantics
- Hand-off and “speaking for” are obtained as a consequence
  - “speaking for” is representation on all formulas
A hospital $H$ allows a patient $A$ to access her records

$$\varphi = \text{says}_{l(H)} P_A(\text{access}(A, A))$$

Suppose the patient listens to music. Is that permitted?

Permission as provability

- **Positive permission:**
  - Is $\varphi \Rightarrow \text{says}_{l(H)} (\neg O_A \neg \text{music})$ provable?

- **Negative permission:**
  - Is $\varphi \Rightarrow \text{says}_{l(H)} O_A \neg \text{music}$ not provable?
Parents (A) should not let their children (B) play by the road

Possible interpretations:

- **Positive permission:** A should not give permission to play
  - Too weak?
- **Negative permission:** A should tell B not to play
  - Arguably, adequate
- **A should physically prevent B from playing**
  - Too restrictive?

In the regulated setting

If B plays by the road, who is to blame: A or B?
Saying is crucial for the analysis

A hospital \((H)\) permits patients \((A)\) to permit their family \((B)\) to access their information

- \(H\) says that \(A\) is *permitted to say* that \(B\) is permitted to access
  - \(\text{says}_{I(H)} \mathcal{P}_A \text{says}_{I(A)} \mathcal{P}_B \text{access}(A, B)\)
- Now, when \(A\) gives permission
  - \(\text{says}_{I(A)} \mathcal{P}_B \text{access}(A, B)\)
- We should be able to infer that \(H\) permits access to \(B\)
  - \(\text{says}_{I(H)} \mathcal{P}_B \text{access}(A, B)\)
- In other words, \(A\) represents \(H\) on \(\text{access}(A, B)\).
Introduction and motivation  System Architecture  Inference component  Policies and conformance  Examples

System architecture

Laws:
1. If B says p, then p
2. p

Utterances:
Law 1 says p
Law 2 says p

Grant or Deny
Violations
Request

Access control: is a request permitted by utterances?
Conformance: do actions satisfy obligations in utterances?

Utterances and conformance

Evaluation of policies yields a set of utterances

State
Axioms
Logic of saying and obligation

Syntax of $L$

\[
\varphi ::= \alpha | \varphi \land \varphi | \neg \varphi | \text{says}_I \varphi | \text{says}_I(y) \varphi
\]

\[
\psi ::= \varphi | \psi \land \psi | \neg \psi | \mathcal{O}_y \varphi
\]

- Atomic predicates: $\alpha = p(y_1, \ldots, y_j)$
  - Predicates are applied to objects or variables: $y_i \in X \cup O$
  - E.g. access($A$, $B$) - access of $A$’s medical records by $B$
- Saying is parameterized on a set of laws
- Syntax enforces alternation between saying and obligation
Axiomatization

**A1** All substitution instances of propositional tautologies.

**A2** \( Q(\varphi \Rightarrow \psi) \Rightarrow (Q(\varphi) \Rightarrow Q(\psi)) \) (for all modalities \( Q \))

**A3** \( \text{says}_{Id} \varphi \Rightarrow \text{says}_{Id'} \varphi \) (for all \( Id \subseteq Id' \))

**A4** \( O_A \varphi \Rightarrow P_A \varphi \) (for all \( A \in O \))

**A5** \( \text{says}_{Id_A} (P_B \text{says}_{Id_B} \varphi) \Rightarrow (\text{says}_{Id_B} \varphi \Rightarrow \text{says}_{Id_A} \varphi) \) (for all \( \{A, B\} \subseteq O, \ Id_A \subseteq I(A), \text{ and } Id_B \subseteq I(B) \))

**A6** \( \text{says}_{Id_A} (P_B \text{says}_{Id_A} \varphi) \Rightarrow \text{says}_{Id_A} \varphi \) (for all \( \{A, B\} \subseteq O, \text{ and } Id_A \subseteq I(A) \))

**R1** From \( \vdash \varphi \Rightarrow \psi \) and \( \vdash \varphi \), infer \( \vdash \psi \)

**R2** From \( \vdash \varphi \), infer \( \vdash Q(\varphi) \) (for all modalities \( Q \))
Decidability

Provability is decidable for the propositional case
For all $\varphi \in L$, $\vdash \varphi$ is decidable

Complexity
- Satisfiability checking is NEXPTIME-complete
- A variant of axioms A5, A6 allows PSPACE satisfiability
  - A strictly larger set of formulas is provable
  - Open question: is it adequate in access control applications?
A policy is a collection of statements:

$\{(id) \varphi \mapsto \psi\}$

- Each statement has a unique $id$.
- Preconditions $\varphi \in L_\varphi$:
  - Obligations must be in the scope of saying.
- True preconditions must have true postconditions.
- Postconditions may make more preconditions true.
States and assignments

State
- Objects known to the system
- Interpretation of predicates w.r.t. objects
- Example:
  - Objects: A, B, C, d
  - Predicates: patient(A), patient(B), relative(A, C), access(B, C), test(B, d)

Evaluation of ground formulas
- Policies are evaluated in a given state
- Assignments map variables in the formula to objects
The first step in checking conformance is to determine what has been said.

Utterance is a nugget of saying

\[ \nu(\text{says}_{id}\psi, S) \]

- Policy contains \((id) \varphi \rightarrow \psi\)
- \(S\) is a state, \(\nu\) is an assignment

Utterance pairs \((U, U')\)
- Utterance set \(U\) corresponds to true preconditions
- Utterance set \(U'\) corresponds to non-false preconditions
Computing utterances (I)

Evaluation of preconditions

- Evaluation is up to an utterance pair: $\text{tv}_{(U,U')}(\varphi, S, v)$
- Interesting case: the saying modality

$$
\text{tv}_{(U,U')}(\text{says}_{id} \psi, S, v) = \begin{cases} 
\top & \text{if } U \models v(\text{says}_{id} \psi, S) \\
\bot & \text{if } U' \not\models v(\text{says}_{id} \psi, S) \\
? & \text{otherwise}
\end{cases}
$$

Consistent utterance pair $U \subseteq U'$

For all policy statements (id) $\varphi \leftrightarrow \psi$

- If $v(\text{says}_{id} \psi, S) \in U$, $\text{tv}_{(U,U')}(\varphi, S, v) = \top$
- If $v(\text{says}_{id} \psi, S) \not\in U'$, $\text{tv}_{(U,U')}(\varphi, S, v) = \bot$
Computing utterances (II)

Fixed point computation
- Initialization: $U = \emptyset, U' = \text{utterances for all postconditions}$
- Computation step:
  - Compute $tv(U, U')$ for all preconditions
  - Add utterances whose preconditions evaluate to $\top$ to $U$
  - Remove utterances whose preconditions evaluate to $\bot$ from $U'$
- Stop when fixed point is reached

Correctness
- The partially ordered set of consistent utterances has a least fixed point
- Computation is monotonic
Conformance is satisfaction of obligations

- **A conforms to the laws** $Id$:
  
  $$\text{If } S \models_{(U,U')} \text{ says}_{Id} \mathcal{O} \varphi, \text{ then } S \models_{(U,U')} \varphi$$

Access control is permission by the laws of the owner

- **A can perform an action** $p$ controlled by $B$
  
  $$S \models_{(U,U')} \text{ says}_{l(B)} \mathcal{P} \varphi$$
## Conformance with nested deontic modalities

**Example**
- Owners of parking lots must forbid parking by lot entrance
- Our interpretation:
  - Owners of parking lots must introduce rules that forbid parking near lot entrance
  - \((P)\) \(\text{owner}(x) \land \text{driver}(y) \rightarrow \mathcal{O}_x \text{says}_{l(x)} \mathcal{O}_y \neg \text{pk}(y, x)\)

**Conformance**
- If an owner \(A\) does not introduce any rules and \(\text{pk}(B, A)\)
  - \(B\) conforms to \((P)\) but \(A\) does not conform to \((P)\)
- If \(A\) introduces \(\text{driver}(y) \rightarrow \mathcal{O}_y \neg \text{pk}(y, A)\)
  - \(A\) conforms to \((P)\) but \(B\) does not conform to \((P)\)
A more elaborate example

Health Insurance Portability and Accountability Act (HIPAA)

- Regulates the uses and disclosures of health information
- Hospitals have local policies, must be HIPAA compliant
- Users give written consent, also part of the regulation

1. An individual **has a right** to access her PHI, except for:
   - i. Psychotherapy notes;
   - ii. PHI compiled for a legal proceeding; or
   ... 

What is a right?
Our interpretation

1. An individual is permitted to require the hospital to permit to access her PHI, except for:
   i. Psychotherapy notes;
   ii. PHI compiled for a legal proceeding; or
   ...

Let $\varphi(x, y, z) = \text{ind}(x) \land \text{says}_{I(\text{HIPAA})}(y) \land \text{info}(z, x, y)$

(1) $\varphi(x, y, z) \land \neg \text{says}_{\{i, ii\}}(z) \iff$
   $\mathcal{P}_x \text{says}_I(x) \mathcal{O}_y \text{says}_I(y) \mathcal{P}_x \text{access}(x, z)$
Hospital and user policies

**Conformant policies**

- A permissive hospital: $\top \mapsto \mathcal{P}_{A\text{access}}(A, r)$
- A hospital who only wants to give access when HIPAA requires it:
  - $\top \mapsto \mathcal{P}_{\text{HIPAA says}_I(\text{HIPAA})} \mathcal{O}_{H\text{ says}_I(H)} \mathcal{P}_{A\text{access}}(A, r)$
  - $H$ permits HIPAA to require it to permit $A$ to access.

**HIPAA consent forms**

- $\top \mapsto \mathcal{O}_{H\text{ says}_I(H)} \mathcal{P}_{A\text{access}}(A, r)$
- Registrars care only about obligations imposed by the hospital

Happy end: $\text{says}_{(H)} \mathcal{P}_{A\text{access}}(A, r)$ is derived
Conclusions

- Logic to represent regulatory documents
  - permission, obligation, cross-referencing
  - multiple sources of authority
- Aimed at checking conformance
  - conformance is decidable and reasonably efficient in practice
- Cross-references can be compiled away for acyclic regulation
  - lose traceability (counterexample generation)
- Designed with NLP in mind
  - Parser is work in progress