

A calculus for access control in distributed systems

M. Abadi, M. Burrows, B. Lampson, G. Plotkin

Kumar Avijit

15-819 Logics and Languages for Security
September 19, 2007

Motivation

- ▶ Access control deals with the relations between principals and resources.
- ▶ Distributed setting brings up interesting modes of interaction.
- ▶ Can the concepts of principals and their interaction with resources be logically motivated?

Motivation - Principals

Many different things qualify as a principal in a distributed setting.

- ▶ A user, an actual machine, or the communication channel?
- ▶ Conjunction, disjunction of principals.
- ▶ Principals may adopt roles.
- ▶ Capabilities may be attached to groups, instead of a single principal.
- ▶ Principals may delegate authority.

Motivation - Access control

The basic questions are:

- ▶ Who is speaking? - Authentication.
- ▶ Is A to be trusted on what he speaks? - Authorization.

Is there a theory that helps decide the authorization question?

Contributions

- ▶ Gives a calculus of principals.
 - ▶ Identifies the primitive constructs, and constructs others.
- ▶ Gives a semantics for the principals' statements.
- ▶ Gives a logical language to express access-control lists.
- ▶ Studies the access-control problem.

Calculus of principals: Informal reasoning

We would like to model common compositions like

- ▶ **Conjunction:** If $A \wedge B$ say something, then both A and B say it.
- ▶ **Disjunction:** Dual to conjunction, turns out this notion indicates a group.
- ▶ **Group membership:** If A is in group G , then A *speaks for* G .
- ▶ **Roles:** A *as* R .
- ▶ **On behalf of:** Two notions!
 - ▶ $A|B$
 - ▶ A *for* B

A says s

- ▶ *says* captures the intent of the principal.
 - ▶ e.g. Bob *says* “Delete foo.bar”
- ▶ The statement *s* may be imperative or factual.
 - ▶ e.g. Server *says* “Bob’s key is K”

The paper does not distinguish these modalities.

[Can an imperative statement be a proposition?]

A useful derived form:

$$A \text{ controls } s \equiv (A \text{ says } s) \supset s$$

The ACL can then be a collection of axioms of the form
A controls s.

Calculus of principals - Intuition

Note that \wedge is associative, commutative, and idempotent.
Qualifies as a meet operator.

Principals form a semilattice under conjunction.

[Why not a lattice? What happens to the following absorption laws?]

- ▶ $A \wedge (A \vee B) = A, A \vee (A \wedge B) = A.$
- ▶ What does the lattice partial order mean intuitively?
 - ▶ If $A \leq B$, then A suffices to sign for both.
 - ▶ Thus B can be thought to be a group with a member A .
 - ▶ This intuition coincides with the $A \vee B$ being thought of as a group with sole members A and B .
- ▶ $A \Rightarrow B$ is then an abbreviation for $A = A \wedge B$.
 - ▶ **[Also verify that alternatively: $B = A \vee B$].**

Calculus of principals - Intuition

What about the “speaks on behalf of” composition? Defined as:
 $B|A$ says s if B says A says s .

- ▶ Principals form a semigroup under $|$.
 - ▶ $|$ is associative. $[A|(B|C) = (A|B)|C]$.
- ▶ $|$ distributes over \wedge .
 - ▶ $A|(B \wedge C) = A|B \wedge A|C$.
 - ▶ $(A \wedge B)|C = A|C \wedge B|C$.

Other operators on principals

- ▶ We can add a unit principal 1 to the semigroup.
 - ▶ $1|A = A$: 1 is an honest principal.
 - ▶ $A|1 = A$: [???].
- ▶ Disjunction operator turns a distributive semilattice into a distributive lattice.
- ▶ Other extensions like generalizing the lattice operations to an infinite case (Quantaes).

A logic of principals - Syntax

Modal logic of principals, with *says* as the modality. Syntax:

Formulae	$s ::= p$	Primitive propositions
	$\neg s$ $s_1 \wedge s_2$	
	$P \text{ says } s$	
	$P_1 \Rightarrow P_2$	
Principal Expressions	$P ::= A$	Basic principals
	$A_1 \wedge A_2$	
	$A_1 A_2$	

A logic of principals - Axioms

$$\frac{s \text{ is a tautology in propositional logic}}{\vdash s}$$

$$\frac{\vdash s \quad \vdash (s \supset s')}{\vdash s'}$$

$$\vdash A \text{ says } (s \supset s') \supset (A \text{ says } s \supset A \text{ says } s')$$

$$\frac{\vdash s}{\vdash A \text{ says } s}$$

Other axioms connecting calculus of principals to logic:

$$\vdash (A \wedge B) \text{ says } s \equiv (A \text{ says } s) \wedge (B \text{ says } s)$$

$$\vdash (B|A) \text{ says } s \equiv B \text{ says } A \text{ says } s$$

$$(A \Rightarrow B) \supset ((A \text{ says } s) \supset (B \text{ says } s))$$

Other relations between principals

- ▶ $A \rightarrow B$, if, for any s , if A says s , then B says s .
 - ▶ Weaker than $A \Rightarrow B$.
- ▶ $(A \text{ says false}) \supset (B \text{ says false})$ abbr. as $A \mapsto B$.
 - ▶ **[A is at least as powerful as B].**
 - ▶ How does this relate to $A \Rightarrow B$?
 - ▶ $A \Rightarrow B$ implies $A \mapsto B$, but not the converse.

Semantics

Kripke Semantics for the modal logic:

$$\mathcal{M} = \langle W, w_0, I, J \rangle$$

- ▶ W is the set of all possible worlds.
- ▶ w_0 is a distinguished world.
- ▶ I maps each proposition symbol to a subset of W .
- ▶ J maps each principal symbol to its accessibility relation ($\subset W \times W$).

Semantics - Accessibility relation

\mathcal{R} extends J to principal expressions

$$\begin{aligned}\mathcal{R}(A) &= J(A) \\ \mathcal{R}(A \wedge B) &= \mathcal{R}(A) \cup \mathcal{R}(B) \\ \mathcal{R}(B|A) &= \mathcal{R}(A) \circ \mathcal{R}(B)\end{aligned}$$

Semantics - Satisfaction

$$\mathcal{E}(p) = I(p)$$

$$\mathcal{E}(\neg s) = W - \mathcal{E}(s)$$

$$\mathcal{E}(s \wedge s') = \mathcal{E}(s) \cap \mathcal{E}(s')$$

$$\mathcal{E}(A \text{ says } s) = \{w \mid \mathcal{R}(A)(w) \subseteq \mathcal{E}(s)\}$$

$$\mathcal{E}(A \Rightarrow B) = W \text{ if } \mathcal{R}(B) \subseteq \mathcal{R}(A), \phi \text{ otherwise}$$

- ▶ $\mathcal{E}(s)$ is the set of all worlds where s “holds”.
- ▶ s holds in \mathcal{M} if it holds at w_0 . $\mathcal{M} \models s$.
- ▶ $\models s$ if s holds in all models \mathcal{M} .

Idempotence

- ▶ We would like to have $|$ idempotent.
 - ▶ Reasonable to assume that $A|A = A$.
 - ▶ Helps preserve rights after hops.
- ▶ Semantics does not validate idempotence.
- ▶ What kind of binary relations force idempotence?

Roles and groups

- ▶ Roles are needed to have a different set of capabilities for different tasks.
 - ▶ Principle of least privileges.
- ▶ Groups induce natural roles, such as G_{role} for a group G .
- ▶ There may be roles corresponding to resources, e.g. one that allows access to a particular directory.

Encoding roles

Assumption: **[Roles can be freely adopted]**.

Define A as R to be $A|R$.

Some desirable features of encoding:

- ▶ $|$ is monotonic in both its arguments. Thus if $A \Rightarrow A'$, $R \Rightarrow R'$, then $A \text{ as } R \Rightarrow A' \text{ as } R'$.
- ▶ $|$ is multiplicative on both sides:

$$(A \wedge B) \text{ as } R = (A \text{ as } R) \wedge (B \text{ as } R)$$

$$A \text{ as } (R \wedge R') = (A \text{ as } R) \wedge (A \text{ as } R')$$

- ▶ We assume $A \Rightarrow (A \text{ as } R)$.

Delegation

What is delegation: The ability of A to give B the right to act on A 's behalf.

Issues:

- ▶ All or none?
Does B get all the rights of A ?
- ▶ Transferability?
Can B delegate the rights to C ?

The framework is rich enough to study various forms of delegation.

Delegation without certificates

Delegation without certificates is easy. Suppose A delegates to B .

- ▶ A request from B on behalf of A would be $B|A$ says s .
- ▶ The access control list would then have an entry for the principal $B|A$.

Delegation with certificates $B \text{ for } A$

- ▶ Suppose D is a delegation server:
 - ▶ For a request B says A says s , D decides if A says s ?
- ▶ Since A is delegating to B , it can say: A says $(B|A \Rightarrow D|A)$.
- ▶ Further, to give A the authority to delegate, we need:
 A controls $(B|A \Rightarrow D|A)$.
- ▶ D need not even exist!

Thus we get $B \text{ for } A = (B \wedge D)|A$.

We can abbreviate $(B|A \Rightarrow D|A)$ as B serves A .

Note that if B serves A , then $B|A \Rightarrow B \text{ for } A$.

$for = | + Delegation.$

Some favourable properties

- ▶ *for* is monotonic in both arguments.
- ▶ *for* is multiplicative in both arguments.
- ▶ *serves* is antimonotonic in second argument.

If C serves A , then $B \wedge C$ serves A .

Summary

- ▶ Vague concepts like assertions, principals, roles and delegations can be given a mathematical meaning.
- ▶ Proposed logical system does not seem to have a good proof theory. A judgmental approach might yield better results than an axiomatic one.