

Delegation Logic by Li et al.
LLSEC, CMU

Sicun(Sean) Gao

10-1-2007

Outline

D1LP (*first version* of DLP(delegation logic program))

- ▶ Concepts and Motivation
- ▶ Syntax
- ▶ “Semantics”
- ▶ Properties

Motivation

- ▶ Authorization in decentralized scenarios:
 - ▶ interacting entities with equally important resources
 - ▶ resource owner and requester are unknown to *each other*
 - ▶ third parties are trusted only for certain things and to certain degrees
 - ▶ access control decisions should be based on *attributes* of subjects

Attributes

- ▶ Attributes should allow following methods
 - ▶ decentralization: for any entities A,B, A can assert B has a certain attribute (truly or wrongly)
 - ▶ delegation: A delegates the authority over an attribute to another B
 - ▶ inference and conjunction of attributes
 - ▶ **attribute-based delegation**: essential for distributed authentication - *stranger's* trustworthiness is based on attributes
 - ▶ attribute with fields: e.g., age or credit limit apply to certain attributes
 - ▶ (optional) delegation with threshold structure

D1PL is claimed to have...

- ▶ *declarative semantics*
 - ▶ "The basic requirement is that a TM language should have a declarative clearly specified notion of proof of compliance" (confusing semantics with proof system)
- ▶ tractability: compliance checking is polynomial in size of input policies etc.

critique before formalization

- ▶ The paper gives a programming/database language and its compilation, not a logic.
 - ▶ *Semantics* is *defined* by translation between D1PL to OLP (Ordinary Logic Programs, plain prolog-ish programs).
 - ▶ Meta-theorems simply do not come into existence.
- ▶ The underlying logic tries to act like a restricted fragment of first order logic without quantifiers, but contains modal operators (*say, delegate, represent*) that are not interpreted modally - cost is, propositions governed by modal operators can not be interpreted as truth-valued. This makes the logic so restricted that it'll be surprising if its proof search isn't tractable.

We'd better only focus on its treatment of key concepts like *delegation*, rather than problems with the whole *logic*.

Syntax

- ▶ full list on paper P139
- ▶ rule ::= head-stmt | head-stmt "if" body-formula (baby implication and conjunction)
- ▶ query ::= body-formula "?" (difference between "head" and "body" is the latter allows compound principals)
- ▶ three key predicates:
 - ▶ A **says** BA
 - ▶ A **delegates** BA^n to B
 - ▶ A **represents** B on BA

Assertion

- ▶ “X says ba” simply means that “X supports the proposition encoded in ba.”
- ▶ Note that conjunctions for principals are allowed, but not for base-atoms.

Delegation

- ▶ Delegation depth is the number of re-delegation steps that are allowed; it has limit D and is “*” when D is exceeded.
- ▶ “ X delegates ba^1 to Y ” means if Y supports ba then X supports it as well and there's no more transfer of ba allowed for Y .

Representation

- ▶ Error: “X represent Y” as defined is not confined on a particular base-atom, while in discussion it is.
- ▶ “X representation Y on ba” does not consume delegation depth, and can only be issued by the local principal. Only the trust root are allowed to use representation statement.
- ▶ In the compilation process a representation statement is translated into delegation with depth 0.

Threshold struct

- ▶ static unweighted: $threshold(k, [A_1, \dots, A_n])$ supports a base atom if at least k principals in the list support it.
- ▶ static weighted: $threshold(k, [(A_1, w_1), \dots, (A_n, w_n)])$ supports a base atom if the sum of weight exceeds k .
- ▶ dynamic: $threshold(k, ?X, Prin\ says\ ba)$, e.g. " $threshold(2, ?X, Bank\ says\ isCashier(?X))$ ".

Example

Accessing Medical Records (Page 147, 20/44)

Tractable translation

The paper gives compilation process between D1LP and OLP; all steps consume polynomial time as to size of related input.