Languages for Policy Formulation and Enforcement

P.A. Bonatti

GSS Conference 2013

Brussels, June 2013

European Network for
Social Intelligence

Main goal of this talk

- Discussing requirements for a policy language
- Capitalizing on previous experience
  - Work on computer policies:
  - Access Control (AC) policies
    - Including trust negotiation (TN)
  - Usage control policies
    - Privacy policicies
    - DRM
- With a general GSS perspective

Outline

- What is a policy?
- Policy usage
- Policy language requirements
- A promising technological framework

Privacy and confidentiality policies

- In their simplest form constrain
  - Access to information / knowledge (server's view)
  - Disclosure of information / knowledge (user's view)
    - e.g. when accounts are created, credit card numbers released

Privacy and confidentiality policies

- In their simplest form constrain
  - Access to information / knowledge (server's view)
  - Disclosure of information / knowledge (user's view)
    - e.g. when accounts are created, credit card numbers released
- Based on
  - Properties of the requester
  - Information / knowledge contents
  - The nature of the current transaction / operation
  - Contextual properties (time, place, etc.)

Privacy and confidentiality policies

- In their simplest form constrain
  - Access to information / knowledge (server's view)
  - Disclosure of information / knowledge (user's view)
    - e.g. when accounts are created, credit card numbers released
- Based on
  - Properties of the requester
  - Information / knowledge contents
  - The nature of the current transaction / operation
  - Contextual properties (time, place, etc.)
- Expressiveness needs for policy languages
  - Complex conditions
  - Over all sorts of knowledge and data

Policies for semantic web & social networks

- Access control & information disclosure depend on **metadata** such as:
  - User profiles
  - Relationships between users
    - Friendship
    - Reputation
  - Content classification
  - etc...
- Such metadata are encoded with KR languages
  - RDF / Description logics
  - Rules
  - In perspective, combinations thereof

Policies for enterprise data

- Recent initiatives aimed at applying the LOD paradigm to organization data / knowledge management
- Increasing use of RDF and OWL

Policy processing / usage

- Enforcement
  - Example from Access Control:
  - Given a state (including a user request),
  - Decide whether the request is permitted or denied
  - Possibly log request / decision, notify administrator, change policy, start a registration process, ...
- More generally:
  - Given a (partial) description of a state
  - Make a decision & apply it
- Main language desiderata:
  - Flexible and general state / decision representation
  - Directly executable declarative specifications
    - intermediate translations may introduce errors

Policy processing / usage

- Reasoning about policy consequences
- Reasoning about what-if scenarios
  - Reasoning about policy effects
  - Policy formulation, assessment, and tuning
- A tool for agreement
  - Reasoning about policy composition
  - Policies result from independent sources of requirements
  - Multiple stakeholders + laws
  - Society vs individuals
- Main language desiderata
  - Clear, unambiguous semantics
  - Hypothetical reasoning (possibly simplified)

Policy processing / usage

- Policy comparison & negotiation
  - Related to enforcement & reasoning about policies
- A tool for decision making & agreement
  - Should I interact with this organization?
  - Is its policy compatible with my requirements?
  - Can we change our policies and find a mutually satisfactory agreement?
  - Experiences from computer privacy (P3P+IE6, TN, …)
  - Related: How to fulfil a policy (TN)
- Main language desiderata
  - Intentional reasoning
    - for *all* possible states, … (not simply evaluation)
  - Abduction (from goal to fulfilling action)
  - Preferences on how to negotiate, fulfil, ...

Policy processing / usage

- Human readable explanations
  - Formal languages are not familiar to everybody
  - Still a policy should be well understood by all the entities subject to the policy
- A tool for usability & ex-post validation
  - Explain the policy as well as *decisions*
- Main language desiderata
  - Possibility of converting from-to natural language
  - Explain the underlying reasoning
  - With as little human intervention as possible
    - Documentation not aligned to policy
    - Extra costs

Policies in abstract terms

- Suitable for Global System Science at large
- Policies are **mappings** from the **states** of a complex system to **decisions**
  - Aimed at constraining the system's behavior
  - States can be represented as complex pieces of knowledge
    - Discrete *and* continuous, possibly partial
  - Decisions:
    - System behavior should/should not be modified
    - The *policy* should be modified
    - Someone should be notified / a process should start
    - Determine alternatives and priorities
    - Take immediate actions automatically

Candidate policy *languages*

- KR (logic-based) languages are a natural choice
- Clean formal semantics
- Direct, uniform representation of:
  - Support knowledge (states)
    - Possibly *incomplete* knowledge as it frequently happens
  - Behavior constraints
    - Focus on *what* is to be achieved vs. *how*
  - Possible decisions
    - Planning concrete actions to achieve desired goals
- Reasoning engines are available
  - For all the kinds of reasoning mentioned so far

Candidate policy *languages*

- Rule-based languages are currently the best choice
  - [P.B., Datalog for Security, Privacy and Trust, 2011]
  - Datalog extensions
  - Answer Set Programming (ASP)
- Appropriate expressiveness
  - Formally: eg. they can express all PTIME policies
  - Empirically: people write policies as rules
- Higher maturity in relation to
  - Support to default policies
  - Support to abduction and explanations
  - Controlled natural language interfaces
  - Integration with other packages & formats

The case of ASP

- Solid implementations based on DLV and its extensions
  - Highly optimized, production stage
  - Integrated with external systems & formats
    - DBMS for processing large bodies of knowledge/data
    - RDF and OWL reasoners
    - External functions & packages
  - Support to nonmonotonic reasoning
    - Default policies, what-if reasoning, ...
  - Reasoning about alternatives and priorities
    - Preferences, weights
  - The standard engine can handle all kinds of policy usage but explanations
    - The language is amenable to adding an independent explanation engine

Summarizing

- Policy languages need to encode and handle
  - Articulated pieces of knowledge
    - Interoperability with many formats and systems
  - Decisions and countermeasures
  - With a clean, unambiguous semantics
- One policy, many uses
  - Enforcement, analysis, comparison, explanations, ...
  - All should be coherent with the semantics
- Rule-based knowledge representation languages
  - Currently the most appealing choice
  - Expressiveness, maturity, interoperability
  - Direct support to most kinds of policy usage

Some open issues

- Space, time, and *autonomy* of agents
  - Constraining and monitoring behavior over extended periods and across multiple places
  - e.g. usage control, DRM, privacy policy enforcement
    - Delete file *within n days*
    - Copy *at most n times*
    - Don't show this to *third parties*
  - Usability vs expressiveness
    - Some dynamic logics are almost programming languages
    - Error prone, difficult to explain
  - Technical obstacles to enforcement
    - Can't *force* agents to adopt desired behavior
    - Monitoring is difficult and expensive

Some open issues

- A recent innovative approach:
- Integrating traditional enforcement and mechanism design
  - Preventing violations through a system of disincentives based on game theoretic techniques, e.g.:
    - reduce user profiling through competition among service providers
    - reduce monitoring costs via strategic allocation of inspections
  - Improving game efficiency through ad hoc technical enforcement mechanisms
    - Which technical solutions best support in governing global systems?

QUESTIONS/DISCUSSION