EPAL

Michael Carl Tschantz
EPAL

- Enterprise Privacy Authorization Language
  - IBM

- A formal language for describing privacy policies
Outline

• Motivation
• Syntax
• Semantics
• Relating Policies
Privacy Policies

- Customers and regulators expect companies to respect privacy or at least provide a warning when they don't
- Companies must make clear to both customers and employees what privacy guarantees they offer
Privacy Policies

• Currently, most policies are unclear
  – written in natural language (e.g., English)
    or worse (Legalese)

• Not usable by computers
  – Which should be configured to obey the policy
EPAL

- Attempts to formalize privacy policies in a machine readable format
- Handles data privacy (flows of information)
  - Most relevant to computers
  - Similar to access control
Outline

• Motivation

• Syntax

• Semantics

• Relating Policies
Rules

- A policy is a list of rules
- In XML
Rules

- “A doctor may view medical records.”
- (doctor, view, medical records, allow)
Rules

- “A doctor may view medical records.”
- (doctor, view, medical records, allow)

Principal

The type of entity requesting access
Rules

• “A Doctor may view medical records.”
• (doctor, view, medical records, allow)
Rules

- “A doctor may view medical records.”
- (doctor, view, medical records, allow)

Data-object
The type of data requested
Rules

• “A doctor may view medical records.”
• (doctor, view, medical records, allow)

Decision
If such requests should be allowed or denied
Purpose

• “A Doctor may view medical records for treatment.”

• (doctor, view, medical records, treatment, allow)
Purpose

• “[Access-control] policies define which subjects can access which objects [for which actions]. Privacy control, however, is usually not concerned with individual users. A customer releases his data to the custody of an enterprise while consenting to the set of purposes for which the data may be used.”

  – Karjoth & Schunter, “A Privacy Policy Model for Enterprises”
Conditions

• “A doctor may view medical records for treatment if data-subject is his patient.”

• (doctor, view, medical records, research, principal = doctor(owner(data-object)), allow)
Obligations

- “A doctor may view medical records for treatment if data-subject is his patient and he logs the access.”
- (doctor, view, medical records, research, principal = doctor(owner(data-object)), logs access, allow)
Rules

- (principal, action, data-object, purpose, conditions, obligations, decision)
- (call center, read, phone number, marketing 9:00am < time < 5:00pm, logs, allow)
- (call center, read, phone number, marketing opt-out(owner(data-object)), logs, deny)
- (IT, record, IP-address, network analysis true, delete no later than in a week, allow)
Policies

• A list of rules

• Rules listed in order of priority
  – First applicable rule trumps all others

• If no rules apply, Not-Applicable is the decision
Policies

• “The call center may read phone numbers from 9:00am to 5:00pm of people who did not opt-out provided they log their access.”

• 1 (call center, read, phone number, opt-out(owner(data-object)), log, deny)

• 2 (call center, read, phone number, 9:00am < time < 5:00pm, log, allow)
Requests

• A request lists a principal, action, data-object, purpose, and containers

• Containers holds facts for proving conditions and may come from different sources

• Containers must be sufficient to prove or disprove every applicable condition

• A policy is evaluated with respect to a request
Vocabularies

• Lists possible values for the principal, data-object, action, purposes, and obligations
• States the format of the containers
• Allows
  − firms to know they are using the same terms
  − systems to know what information is needed for conditions to be evaluated
  − systems to know what obligation it must implement
Hierarchies

- Vocabularies provide a hierarchy of principals
Hierarchies

- Vocabularies provide a hierarchy of data-objects
Hierarchies

- Vocabularies provide a hierarchy of purposes

Marketing
- Telamarketing
- Mailing

Customer Service
- Recalls
- Refunds
Outline

• Motivation
• Syntax
• **Semantics**
• Relating Policies
Semantics

• Take the decision and obligations of the first applicable rule

• If no rule is applicable, return Not-Applicable

• A rule is applicable if it passes the scope check and the provided containers prove its conditions
Scope Check

• An “allow” rule passes the scope check iff
  – the request's principal is the same as the rule's or is a child of the rule's
  – the request's data-object is the same as the rule's or is a child of the rule's
  – the request's purpose is the same as the rule's or is a child of the rule's
  – the request's action is the same as the rule's
Scope Check

- A “deny” rule passes the scope check iff
  - the request's principal is the same as the rule's or is a child or parent of the rule's
  - the request's data-object is the same as the rule's or is or a child or parent of the rule's
  - the request's purpose is the same as the rule's or is a child or parent of the rule's
  - the request's action is the same as the rule's
Scope Check

- Given the request (faculty, a, o, p, [])
  - Fails (professor, a, o, p, true, [], allow)
  - Passes (employee, a, o, p, true, [], allow)
  - Passes (professor, a, o, p, true, [], deny)
  - Passes (employee, a, o, p, true, [], deny)
Rule Semantics

- If a request passes the scope check of a rule, the conditions of the rule are evaluated used the containers of the request.
- If the conditions evaluate to true, the decision of the rule applies.
- Otherwise, the next rule is consulted.
Outline

- Motivation
- Syntax
- Semantics
- Relating Policies
Relating Policies

• EPAL does not provide for policy comparisons or composition

• M. Backes, B. Pfitzmann, M. Schunter
  “A Toolkit for Managing Enterprise Privacy Policies”
Refinement

• The refinement $P'$ may extend a policy $P$ to deal with new cases

• If $P$ is Not-Applicable to a request, then the refinement $P'$ may return anything

• Otherwise, $P'$ must match $P$

• “Doctors and nurses may read medical records” refines “Doctors may read medical records”
Compatible Vocabularies

- The refinement must have a *compatible vocabulary*
  - New principals and sub-principal relations added by the refinement must make sense given the original principals and sub-principal relations
  - New data-objects ... must make sense ...
  - New purposes ... must make sense ...
  - ...

Compatible Vocabularies

• Not Compatible:

Doctor

Physician

Physician

Doctor
Obligation Refinement

- The obligations of the refinement must refine the obligations of the original policy.
- The obligations $o_1$ refines $o_2$ where $o_1 \subseteq V_1$ and $o_2 \subseteq V_2$ iff exists a subset $o$ of $V_1 \cap V_2$ such that $o_1 \rightarrow_1 o \rightarrow_2 o_2$.
Refinement

- A policy $P'$ refines a policy $P$ iff they have compatible vocabularies and for every request $Q$ such $P(Q).\text{decision}$ is not $\text{Not-Applicable}$, 
  - $P'(Q).\text{decision} = P(Q).\text{decision}$ and 
  - $P'(Q).\text{obligations}$ refines $P(Q).\text{obligations}$
Equivalence

• Two policies P1 and P2 are equivalent iff they have compatible vocabs and for all requests Q,
  - $P1(Q)\text{.decision} = P2(Q)\text{.decision}$,
  - $P1(Q)\text{.obligations}$ refines $P2(Q)\text{.obligations}$, and
  - $P2(Q)\text{.obligations}$ refines $P1(Q)\text{.obligations}$

• Theorem: If P1 refines P2 and P2 refines P1, then P1 and P2 are equivalent
Direct Policy Composition

• Two companies want a joint venture that obeys both of their policies

• The composite policy should be a refinement of each company's policy

• Not always possible

• Map conflicts to an Error decision
Ordered Policy Composition

• A department wants to enforce its local policy while always yielding to company's global policy

• The composite policy should be a refinement of the company's policy

• Theorem: If P1 and P2 have compatible vocabularies, then there exists an ordered policy composition of P1 and P2 that is a refinement of P1
Conclusion

• EPAL provides a purpose field unlike access-control languages

• Allows for formal policies to be stated, but since the terms used by the policy have no meaning, it still unclear what it means to enforce the policy