Lecture 12

Friday, 14 October 2022 15:33

purpose specification is important for privacy-aware access control

privacy policy
- who
- conditions
- obligations

EPAL goals
- privacy control (i.e. enable policy enforcement)
- auditing — i.e. seeing whether policies were violated
- transfer of policy-protected data

Not: providing a user interface

EPAL
- formalizes privacy policies
- formalizes privacy options
- manage consent
- enforcement
- audit

traditional access control → doesn't take user preferences into account (at least not nicely)
sticky policy paradigm → ask for consent if not already given

data is transferred along with policy regulating access to it.

vocabulary →
- user hierarchy
- data hierarchy
- action hierarchy
- purpose hierarchy
- obligation model $(O, \rightarrow)$ (obligations)
  - ↑ transitive relation of obligations, where $o_1 \rightarrow o_2$ states that ?

rules $\langle (user, data, purpose, action), (ruling, condition, obligation) \rangle$

privacy policy (vocabulary, ruleset, global condition, default ruling, default obligation)

request (user, data, purpose, action)

policy maps (user, action, purpose, data) + variable assignment to decision + obligations

(policy_error, $\emptyset$) is the response when the global condition is not met

default obligations are only returned when no allow/deny rules match
i.e. when we return the default ruling

EPAL provides
- policy refinement → a policy is a refinement of another policy 2 iff when policy 2 returns {allow, deny}, policy 1 returns the same. (and, when r_2 returns policy_error, r_1 does too; if r_2 = don't care, r_1 gives allow, deny, don't care)
  - and fulfillment of the obligations in refined policy 1 implies obligations in policy 2 are satisfied
  - i.e. there exists $o \in O_1 \cap O_2$ such that $o_1 \rightarrow o \rightarrow o_2$ (according to $\rightarrow_{o_2}$; according to $\rightarrow_{o_1}$)
- policy composition