Lecture 13

Tuesday, 18 October 2022 10:44

XACML defines language to express
- policies
- requests
- responses

as well as an access decision process

policy administration point

policy decision point — evaluates policy + returns access decision

policy enforcement point — enforces decisions

policy information point — source of attributes

attributes are associated with subjects, objects, actions & environment/context

policyset contains policies, which contain rules

target defines where policy is applicable

combining algorithms for policies & rules

target

effect

condition

rule

policy — composed of subcomponents

obligation

<target> contains conjunctive sequence of <anyof>

<anyof> contains disjunctive sequence of <allof>

<allof> contains conjunctive sequence of <match>

<match> defines an atomic access constraint

request specifies attributes of subject/environment/...

∧	1	0	⊥
1	1	0	⊥
0	0	0	0
⊥	⊥	0	⊥

∨	1	0	⊥
1	1	1	1
0	1	0	⊥
⊥	1	⊥	⊥

access decision set: P, D, I, NA

extend indeterminate: I{P}, I{D}, I{PD}

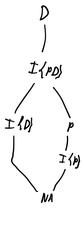
I{P} → I

I{D} → I

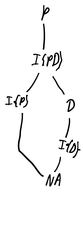
I{PD} → I

I → I{PD}

deny-overrides



permit-overrides



first-applicable — return decision of first applicable policy

i.e. the first one which doesn't return NA

only one applicable
- if 0 sub-rules/policies are applicable, return NA
- if 1 sub-rule/policies are applicable return the result of that rule/policy
- if more than 1 sub-rule/policies are applicable, return indeterminate