CERIAS

the center for education and research in information assurance and security

PSAC: Privilege State based Access Control

Ashish Kamra, Elisa Bertino
akamra@purdue.edu, bertino@cs.purdue.edu

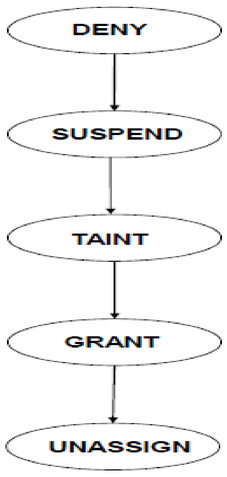
Objective : To support fine-grained decision semantics in an access control system for request suspension and request tainting

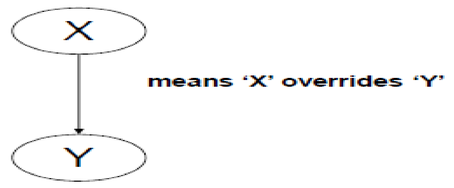
Key Idea : A privilege assigned to a user/role has a state attached to it. Access control enforcement code returns the final state of a privilege .

Privilege state semantics

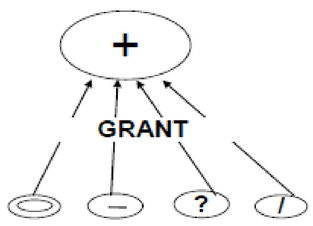
State	Access Check Result Semantics
unassign	The access to the resource is not granted.
grant	The access to the resource is granted.
taint	The access to the resource is granted; the system audits access to the resource.
suspend	The access to the resource is not granted until further negotiation with the principal is satisfied.
deny	The access to the resource is not granted.

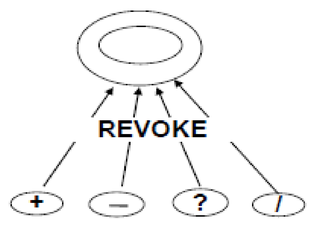
Privilege state dominance relationship for state conflict resolution

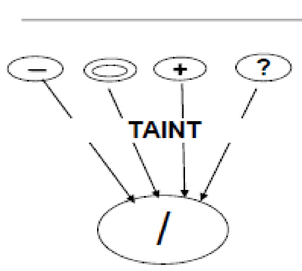


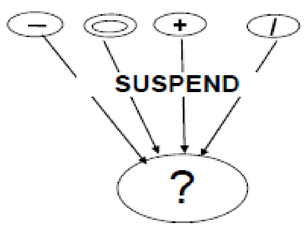


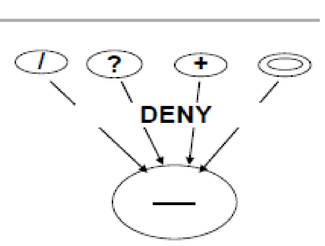
Privilege state transitions



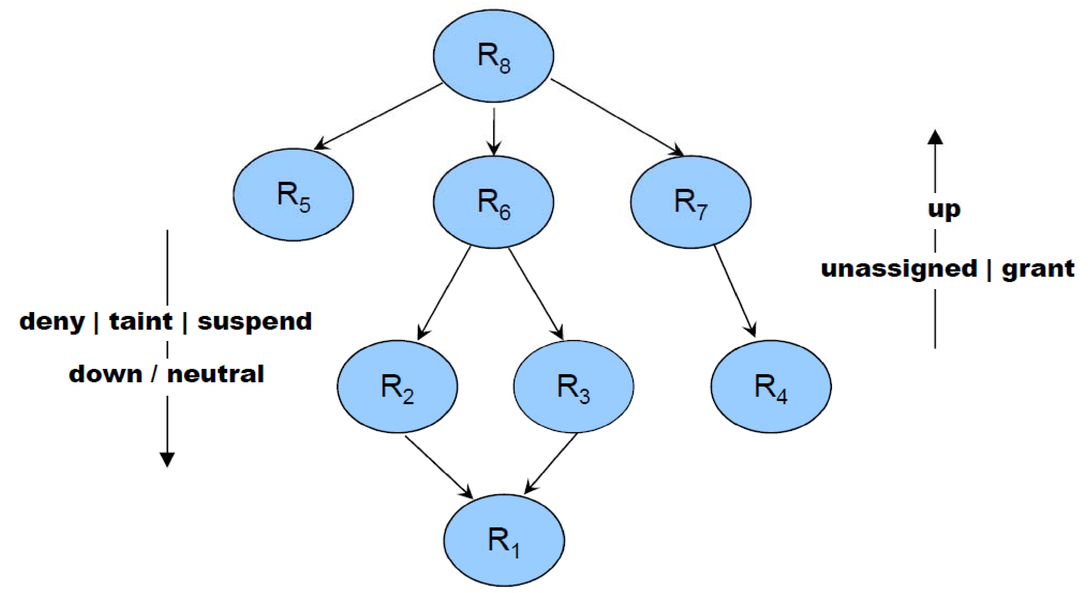








Privilege state orientation in a role hierarchy



- Fine grained decision semantics in PSAC provide system support for an intrusion response system and/or a continuous event-based authentication/auditing system
-Implemented PSAC in the PostgreSQL DBMS as a proof-of-concept.
-Negligible overhead on the access control enforcement code due to privilege states
-Source code available on request

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center