

goal of access control: protect confidentiality + integrity of data/resources from unauthorized access

↳ to be extended for privacy: specify purposes of data

purpose specification

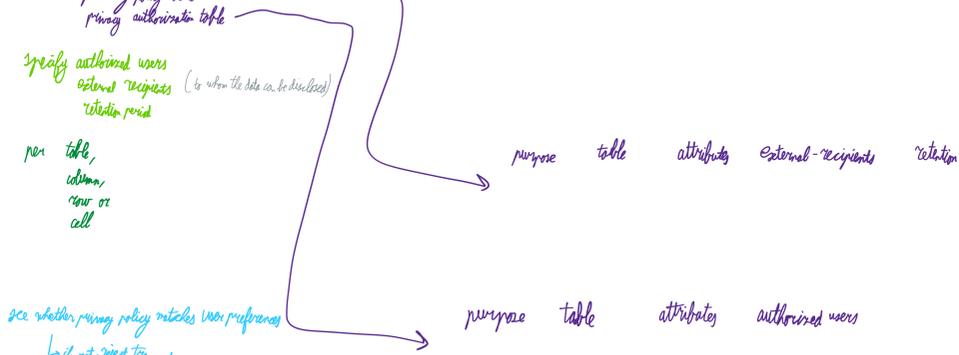


Privacy - aware access control

↳ access decision based on purpose

purpose management
 purpose determination
 purpose control (verification)

Hyperstar database: privacy policy based on purpose guides access control to data



queries should include purpose and this should be checked

note: watch out for leaking data through conditions in query
 even if data is not sensitive, some things might be important for whom it's small set

purpose management is difficult in hyperstar databases

while user might not purposely specify a query's purpose...

Purpose-based access control

definition of purpose

purpose compliance

access purpose determination

access purpose (AP) for a given request

intended purpose (IP) for some data

allowed intended purpose (AIP)

prohibited intended purpose (PIP)

$$IP = \langle AIP, PIP \rangle$$

$$P^\uparrow = \text{ancestors}(P)$$

$$P^\downarrow = \text{descendants}(P)$$

$$P^\oplus = P^\uparrow \cup P^\downarrow$$

$$AIP^\downarrow = \bigcup_{aip \in AIP} \text{descendants}(aip)$$

$$PIP^\uparrow = \bigcup_{pip \in PIP} \text{descendants}(pip) \cup \text{ancestors}(pip)$$

$$IP^* = AIP^\downarrow - PIP^\uparrow$$

$$AP \Leftarrow_{PI} IP \quad \text{iff} \quad AP \in IP^*$$

$$AP \notin PIP^\oplus \quad \text{and} \quad AP \in AIP^\downarrow$$

data access is allowed only if $AP \Leftarrow_{PI} IP$

purpose will be specified by

- the user → may be undetected
- the application → determined for context (i.e. general-purpose application)
- the context → difficult to consider all possibilities

idea: role attributes can be used to specify purposes

e.g. marketing employees will probably access data for marketing purposes.

note: if a user has a role with a context attribute, they will be assigned (per user) a value for that attribute

system attributes are assigned to environment by system admin

conditional role via $\langle r, c \rangle$

an activated role r belongs to conditional role $\langle r, c \rangle$ if

$$r \in \text{descendants}(r)$$

and c is true

access purpose verification

exercise

access purpose authorization

$$\langle ap, \langle r, c \rangle \rangle$$

in our case, we get

$$ap = \text{service-update}$$

$$r = E - marketing$$

$$c = \text{YearsonCompany} \geq 5 \wedge \text{logged} > 7 \wedge \text{currenttime} \geq 9 \text{ am} \wedge \text{currenttime} \leq 5 \text{ pm}$$

cannot access data in case of question?; roles not sufficiently specific i.e. marketing dept of descendants (E-marketing)