Lecture 11

Tuesday, 11 October 2022 10:38

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 policy: who uses
what data
and how do they use it

obligation

subject
action
object } → access control
purpose
condition
obligation

usage control misses post-obligations and finds it difficult to verify purposes
↑ could be implemented as obligations

privacy-aware access control

↳ access decision based on purpose

purpose management
purpose determination
purpose control (verification)

Hippocratic databases: privacy policy based on purpose guides access control to data

privacy policy table → purpose | table | attributes | external-recipients | retention

privacy authorization table → purpose | table | attributes | authorized users

specify authorized users
external recipients (to whom the data can be disclosed)
retention period

per table,
column,
row or
cell

see whether privacy policy matches user preferences
↳ if not, reject transaction

queries should include purpose and this should be checked

↓

note: watch out for leaking data through conditions in query

even if data is not in result set, some things might be inferred from what is in the result set

purpose management is difficult in hippocratic databases

and the user might not properly 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)

$IP = \langle AIP, PIP \rangle$

$p^{\uparrow}$ = ancestors (p)
$p^{\downarrow}$ = descendants (p)
$p^{\updownarrow} = p^{\uparrow} \cup p^{\downarrow}$

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

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

$IP^{*} = AIP^{\downarrow} - PIP^{\updownarrow}$

$AP \Leftarrow_{pr} IP$ iff $AP \in IP^{*}$

$AP \notin PIP^{\updownarrow}$ and $AP \in AIP^{\downarrow}$

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

purpose could be specified by

the user → may be unreliable
the application → doesn't work for complex (i.e. general-purpose) applications
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 certain attribute, they will be assigned (per user) a value for that attribute

system attributes are assigned to environment by system admin

conditional role is a pair $\langle r, c \rangle$

an activated role r belongs to conditional role $cr_i = \langle r_i, c_i \rangle$ if
$r \in$ descendants (r_i)
and c_i is true

access purpose verification

. . . . .

---

exercise

access purpose authorization
$\langle ap, \langle r, c \rangle \rangle$

in our case, we get
ap = service-update
r = E-marketing
c = YearsInCompany ≥ 5 ∧ ExpLevel > 7 ∧ currentTime ≥ 9am ∧ currentTime ≤ 5pm

cannot access data in case of question 2; role is not sufficiently specific

i.e. marketing-dept ∉ descendants (E-Marketing)