ЗАШТИТА ПОДАТАКА

ЗАШТИТА СИСТЕМА

Заштита помоћу улога

Преглед

- Биће објашњено:
  - Концепт приступа помоћу улога
  - Фамилија концептуалних модела
    - основни модел
    - хијерархија улога
    - ограничења
    - консолидовани модел
  - Модели управљања

Приступ помоћу улога

- Концепт контроле приступа помоћу улога (role-based access control) јавља се са развојем вишекорисничких и вишепрограмских система.
- Централна идеја овог приступа је у томе да се права приступа додељују улогама, а да се корисницима додељују одговарајуће улоге.
- Улоге се креирају за различите позиције у организацијама, а корисницима се додељују улоге на основу њихових одговорности и квалификација.
- Корисницима лако може да се промени улога, а улогама могу да се додају нова права приступа или да им се уклоне постојећа.

Мотивација за увођење оваквог приступа

- Данашњи оперативни системи користе контролу приступа помоћу улога.
- Апликације одавно примењују овај принцип, али самостално, јер на нивоу оперативног система нема довољно подршке за апликативну контролу приступа помоћу улога.
- Таква подршка почиње да се појављује у разним производима.
- Изазов је направити апликацијски независне алате, који су довољно флексибилни, а уједно лаки за имплеметацију, помоћу којих би се могле правити различите апликације које користе овакав приступ

Релације између улога

- Софистицираније варијације контроле приступа укључују могућности релација између улога.
- Тако бисмо могли да имамо улоге које су међусобно искључиве (корисник би могао да буде у само једној од оваквих улога).
- Или би улоге могле да наслеђују права приступа једне од других.
- Овако бисмо релације које би иначе морале да буду дефинисане у софтверу, могли да дефинишемо само једанпут на нивоу домена.

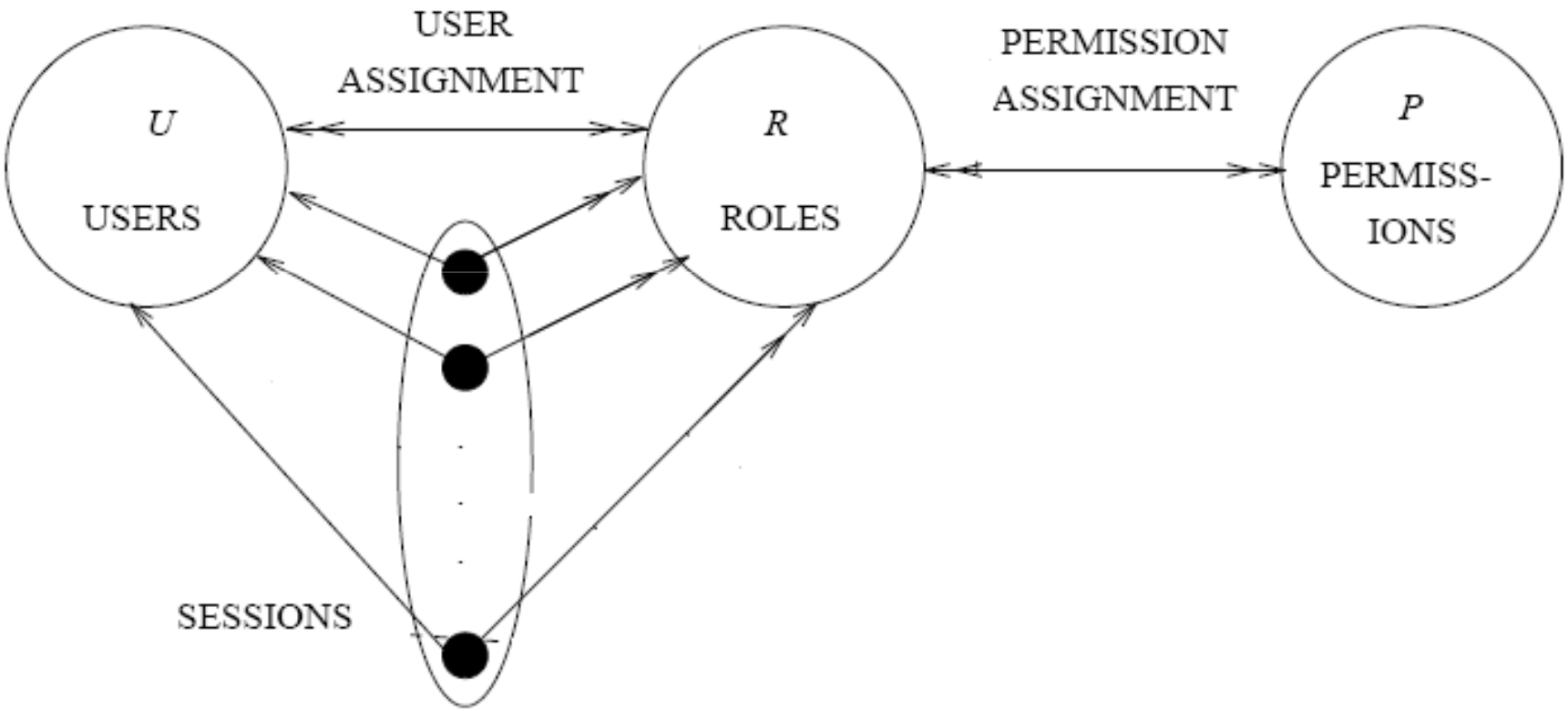
Улоге

- Која је разлика између улога и група?
- групе представљају скуп корисника, а не скуп права приступа
- улоге представљају и скуп корисника, са једне стране, и скуп права приступа, са друге стране
- улога служи као посредник који спаја ова два скупа

Фамилија концептуалних модела

- Да би се објасниле различите димензије контроле приступа помоћу улога, дефинисана су четири концептуална модела:
  - основни модел
  - хијерархија улога
  - ограничења
  - консолидован модел

Основни модел



Основни модел (2)

- састоји се од 3 сета ентитета:
  - корисника (U users) - људско биће (у општем случају може бити и неки аутоматизовани агент)
  - улога (R roles) - назив функције или титула у оквиру организације са неким одговорностима које та функција носи са собом у оквиру организације
  - права приступа (P permissions) - дозвола специфичног приступа неком објекту у оквиру система

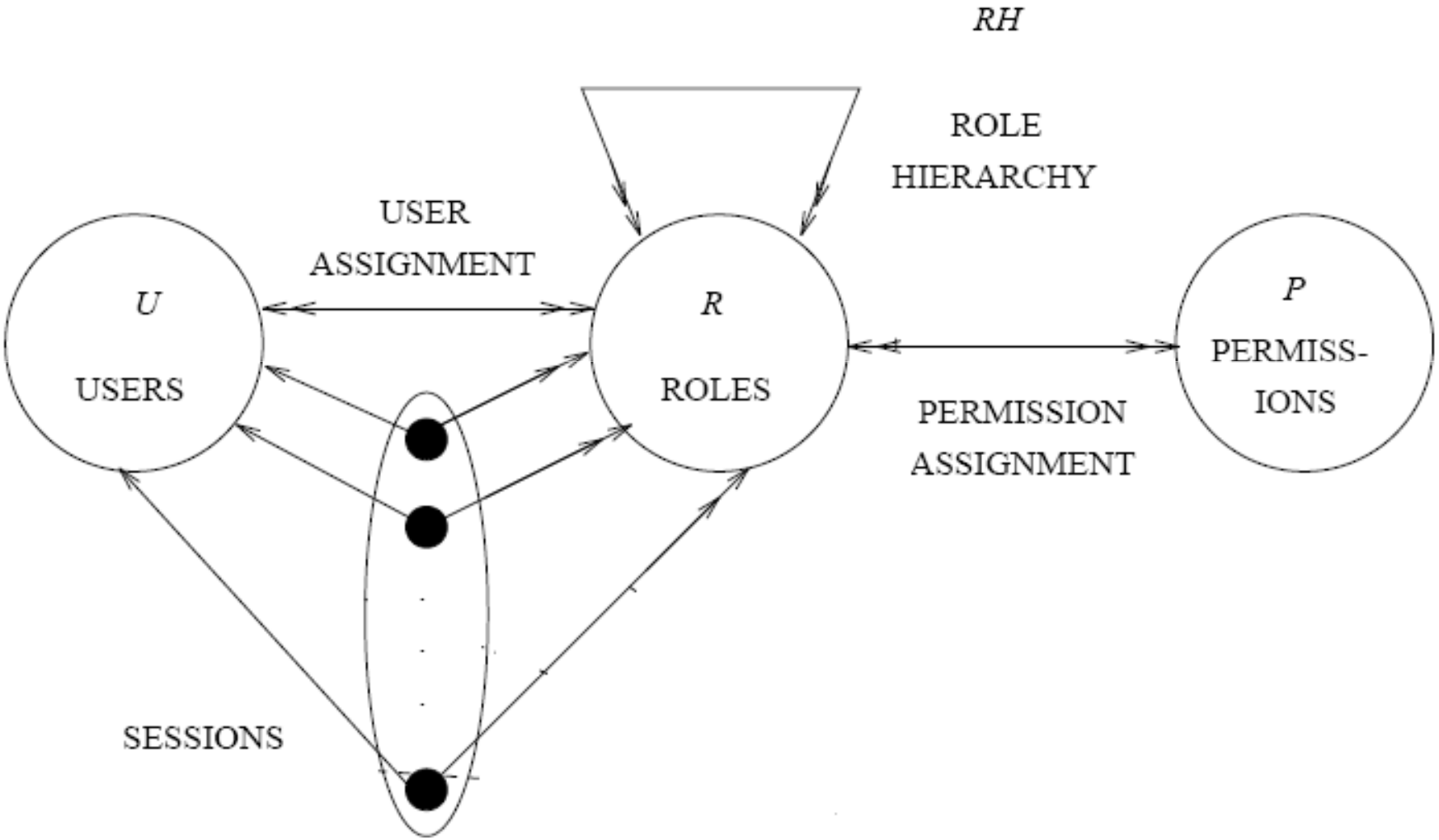
Основни модел (3)

- постоје 2 релације које описују односе између сетова ентитета:
  - додела корисника (user assignment) - више у више веза, корисник може имати више улога, а исту улогу може имати више корисника
  - додела права приступа (permission assignment) - више у више веза, улога може имати више различитих права приступа, а једно право приступа може бити додељено већем броју улога

Основни модел (4)

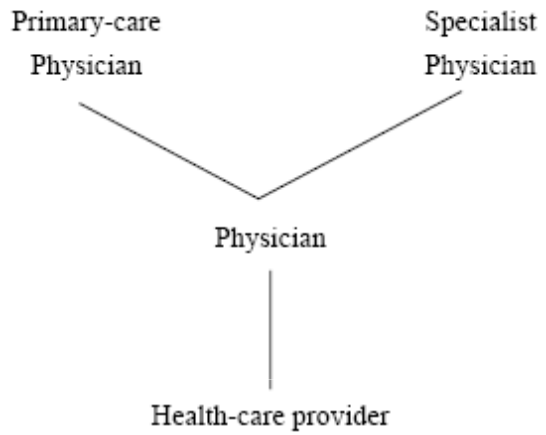
- Свака сесија је релација између једног корисника и једне или више улога.
- Један корисник може да активира више улога чији је он члан.
- У том случају корисник има скуп права приступа, који заправо представља унију скупова права приступа свих улога које је активирао.

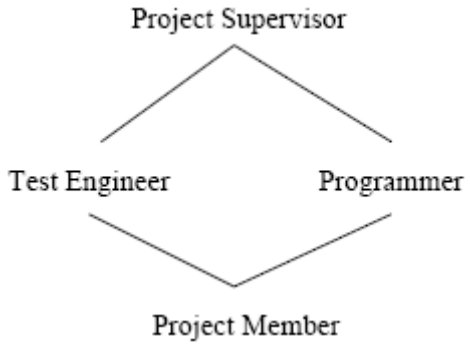
Хијерархија улога



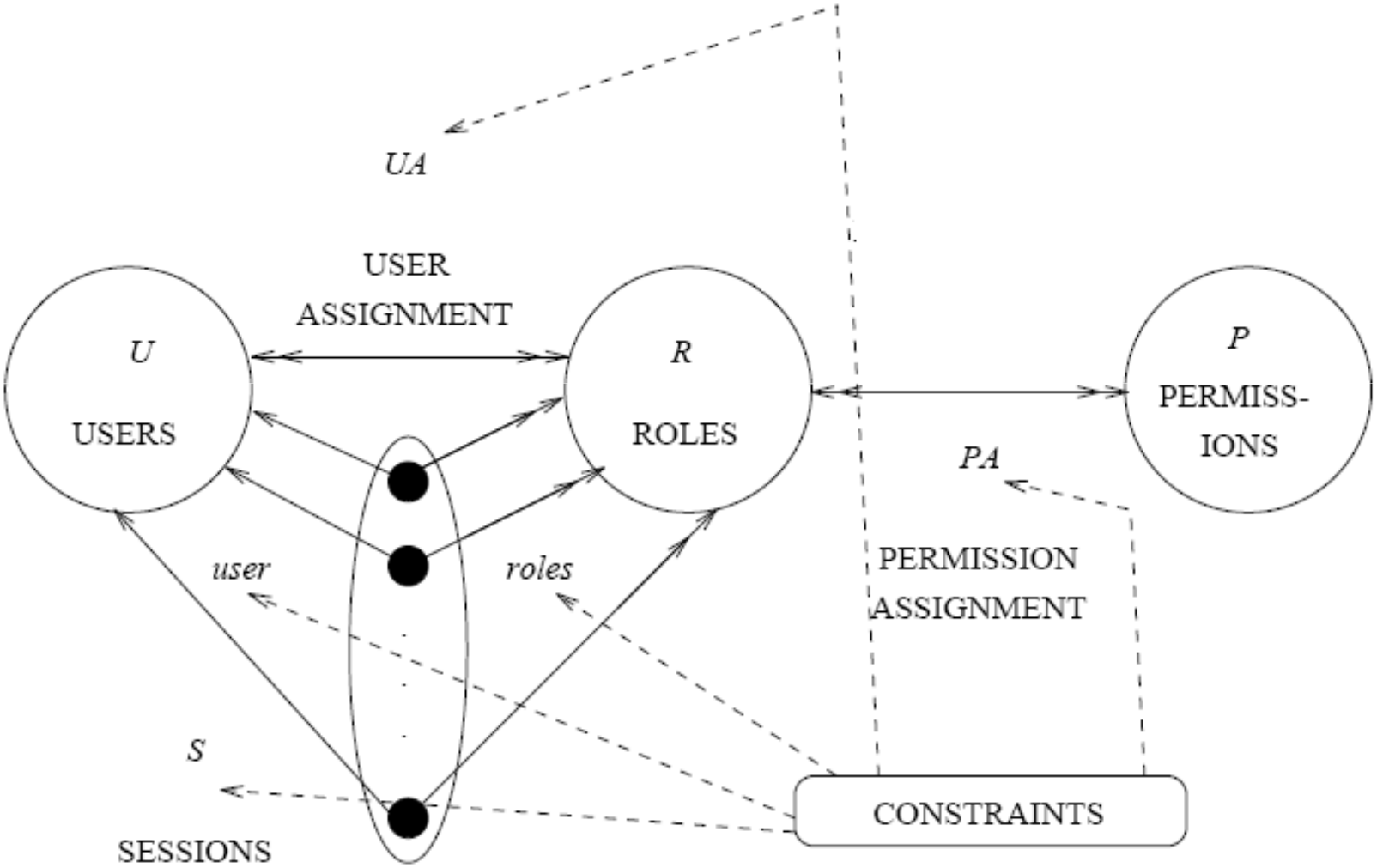
Хијерархија улога (2)

- природно средство за структуирање улога у оквиру организације
- одражава структуру ауторитета и одговорности улога у оквиру организације





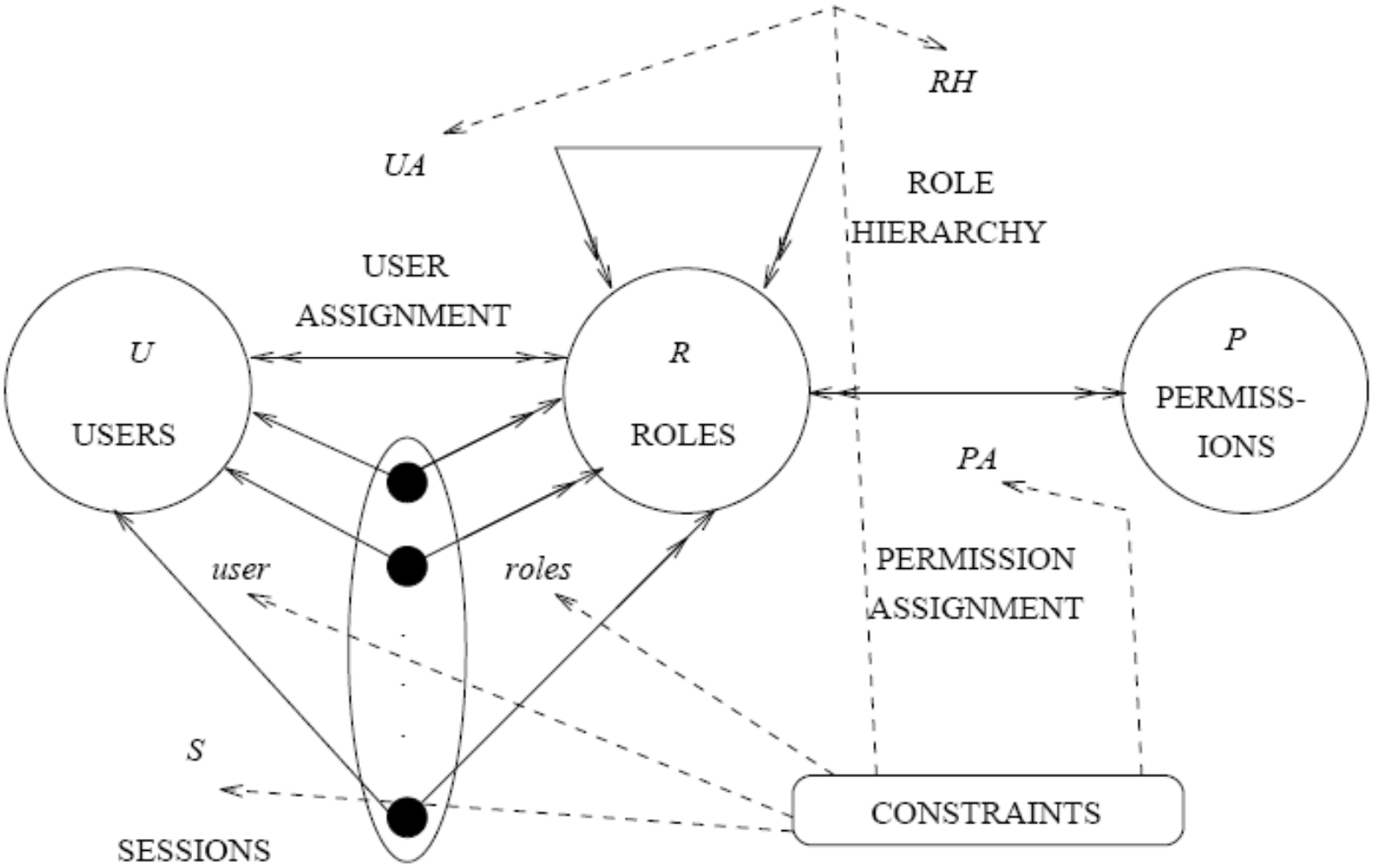
Ограничења


UA
USER
ASSIGNMENT
U
USERS
R
ROLES
P
PERMISS-
IONS
PA
PERMISSION
ASSIGNMENT
user
roles
S
SESSIONS
CONSTRAINTS

Ограничења (2)

- механизам за раздвајање дужности
- нпр. не дозвољава једном кориснику да буде менаџер набавке и финансијски директор у оквиру предузећа (због могућности превара)
- када се две улоге прогласе узајамно ексклузивним, нема више бриге око додела улога корисницима (без овог механизма, морала би оваква ограничења да се уводе програмски или би неко ко је задужен за доделу улога морао да води рачуна о томе)

Консолидовани модел



Консолидовани модел (2)

- комбинује хијерархију улога и ограничења
- ограничења се могу примењивати и на хијерархију улога
- може се ограничити број улога које једна улога може да има изнад или испод себе у хијерархији улога
- може се увести ограничење да нека улога не може да има улоге изнад себе у хијерархији

Модели управљања

- до сада смо претпоставили да контролом приступа помоћу улога управља једна особа
- пошто број улога и корисника у једној организацији може бити изузетно велик, поставља се питање управљања описаним системом
- исти приступ може бити искоришћен за управљање самим собом

Модели управљања (2)