CSC429 – Computer Security

LECTURE 8
ACCESS CONTROL

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Access Control

Role Based Access Control

Role Based Access Control

- Motivating Problem:
  - how to administer user-permission relation

- Roles as a level of indirection
  - Butler Lampson: "all problems in Computer Science can be solved by another level of indirection"

Role Based Access Control (RBAC)

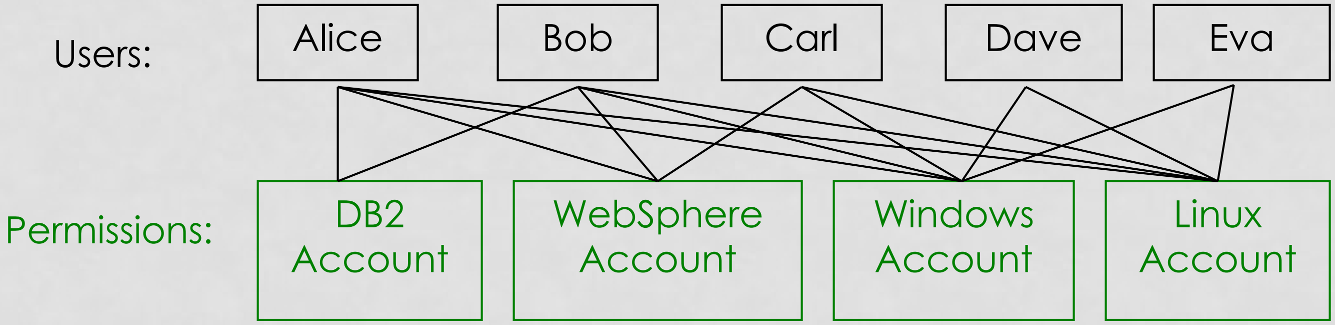
- ACLs do not distinguish between different types of users

- RBAC assigns permissions to specific groups with meaning in the organization, rather than to low level data objects

- Makes administering security easier

RBAC Example

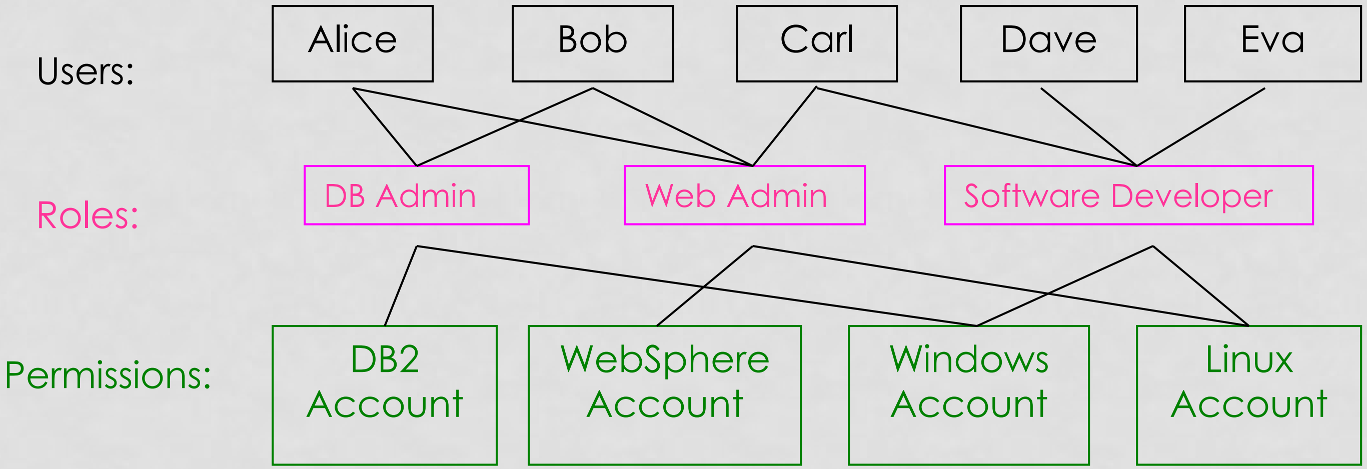
- Non-role-based systems



Users: Alice Bob Carl Dave Eva

Permissions: DB2 Account WebSphere Account Windows Account Linux Account

- RBAC



Users: Alice Bob Carl Dave Eva

Roles: DB Admin Web Admin Software Developer

Permissions: DB2 Account WebSphere Account Windows Account Linux Account

Why Roles?

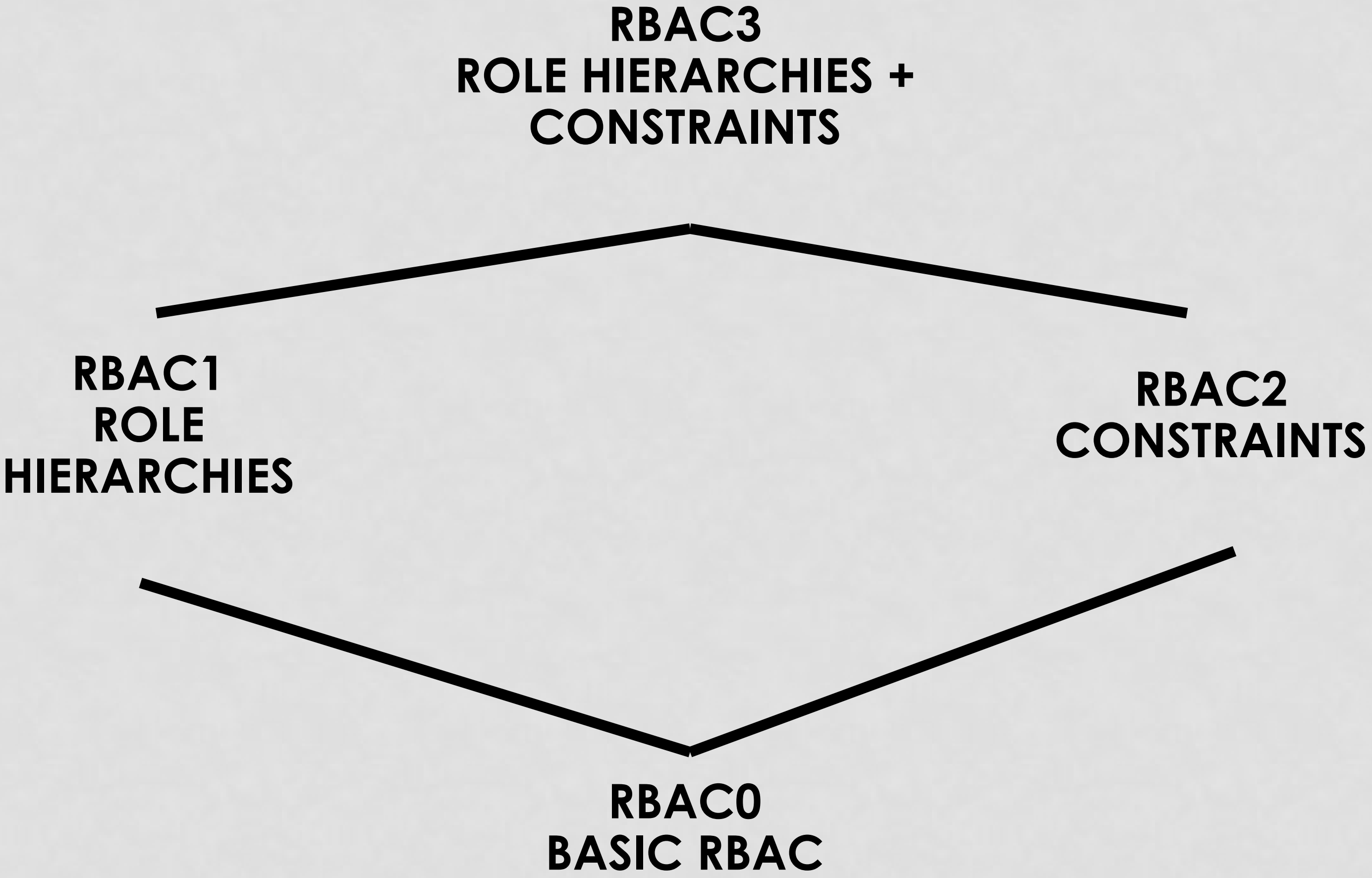
- Fewer relationships to manage
  - possibly from O(mn) to O(m+n), where m is the number of users and n is the number of permissions
- Roles add a useful level of abstraction
- Organizations operate based on roles
- A role may be more stable.

Groups vs. Roles

- Depending on the precise definition, can be the same or different.

- Some differences that may or may not be important, depending on the situation
  - Answer 1: sets of users vs. sets of users as well as permissions
  - Answer 2: roles can be activated and deactivated, groups cannot
    - Groups can be used to prevent access with negative authorization.
    - Roles can be deactivated for least privilege
  - Answer 3: can easily enumerate permissions that a role has, but not for groups

RBAC Models Family



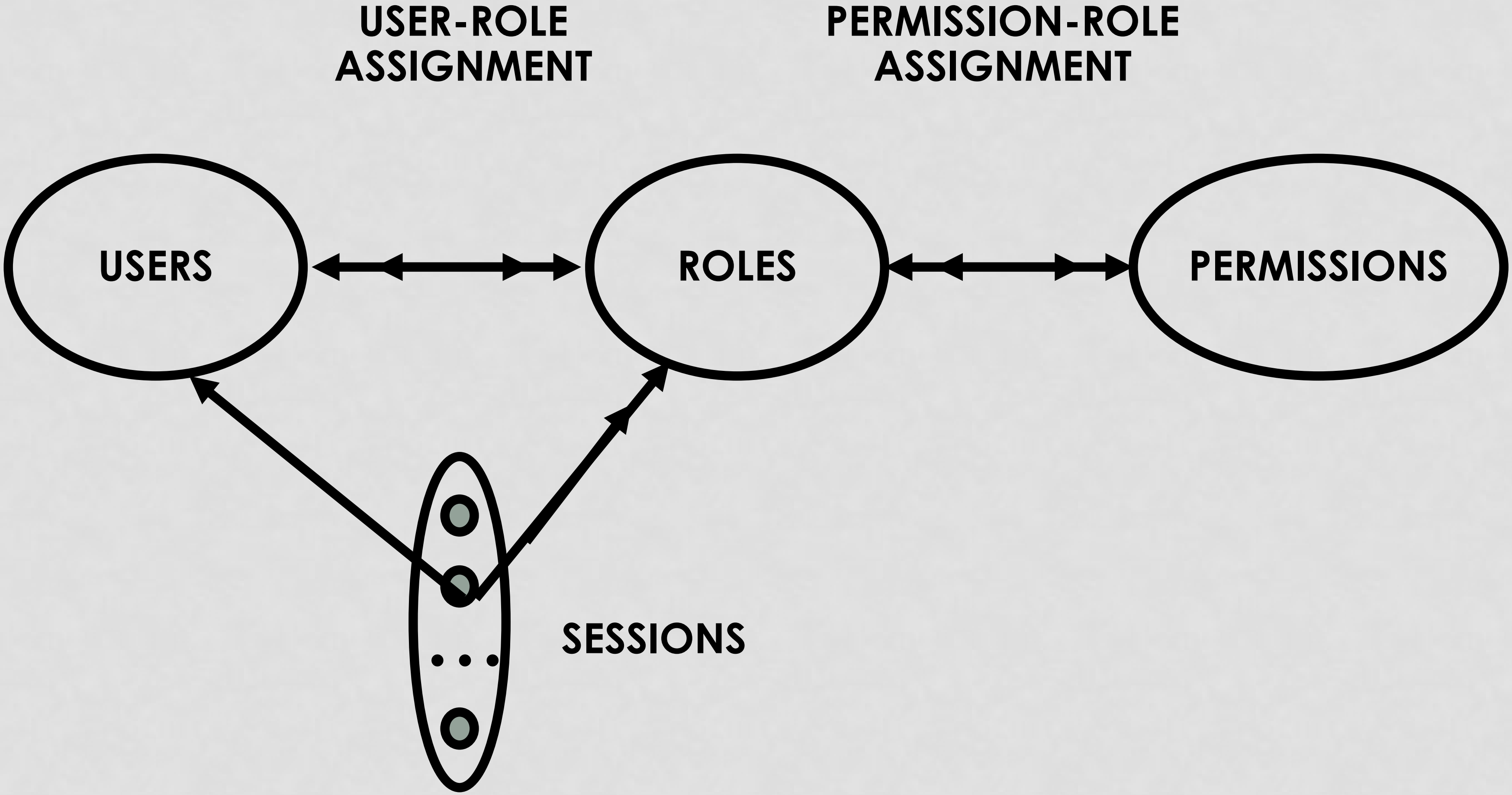
RBAC3
ROLE HIERARCHIES +
CONSTRAINTS

RBAC1
ROLE
HIERARCHIES

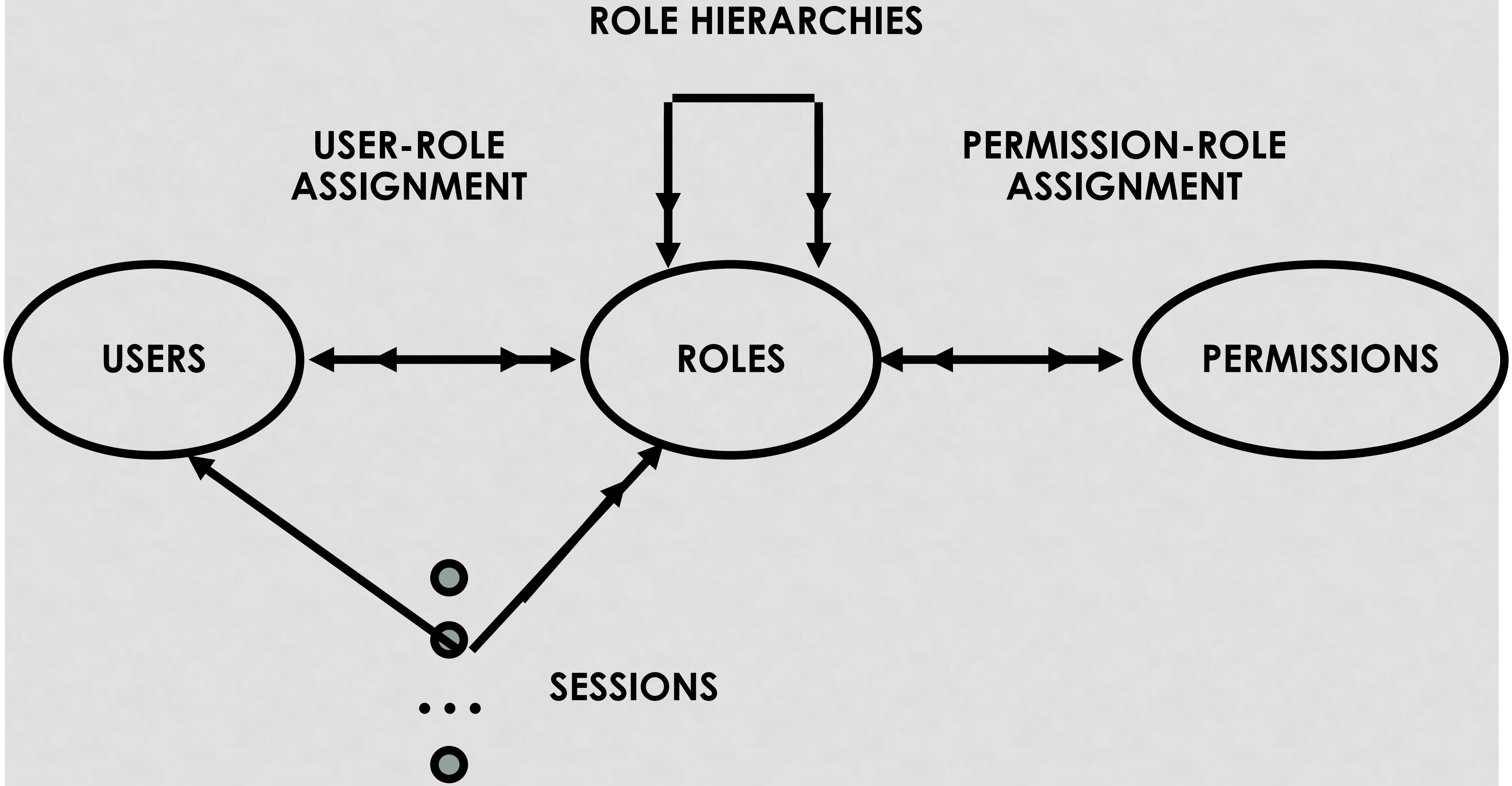
RBAC2
CONSTRAINTS

RBAC0
BASIC RBAC

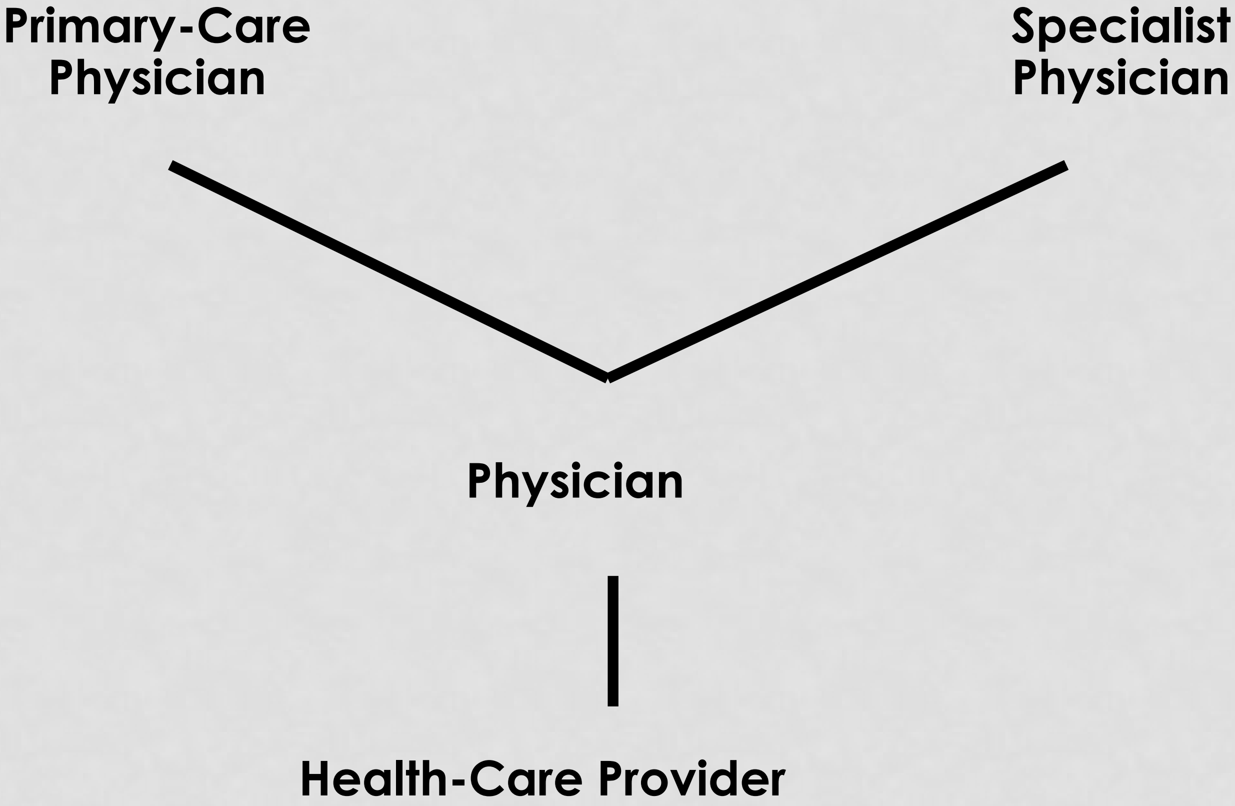
Basic RBAC


USER-ROLE ASSIGNMENT
PERMISSION-ROLE ASSIGNMENT
USERS
ROLES
PERMISSIONS
SESSIONS

RBAC1 (With Hierarchies)



Hierarchal Roles



Primary-Care Physician

Specialist Physician

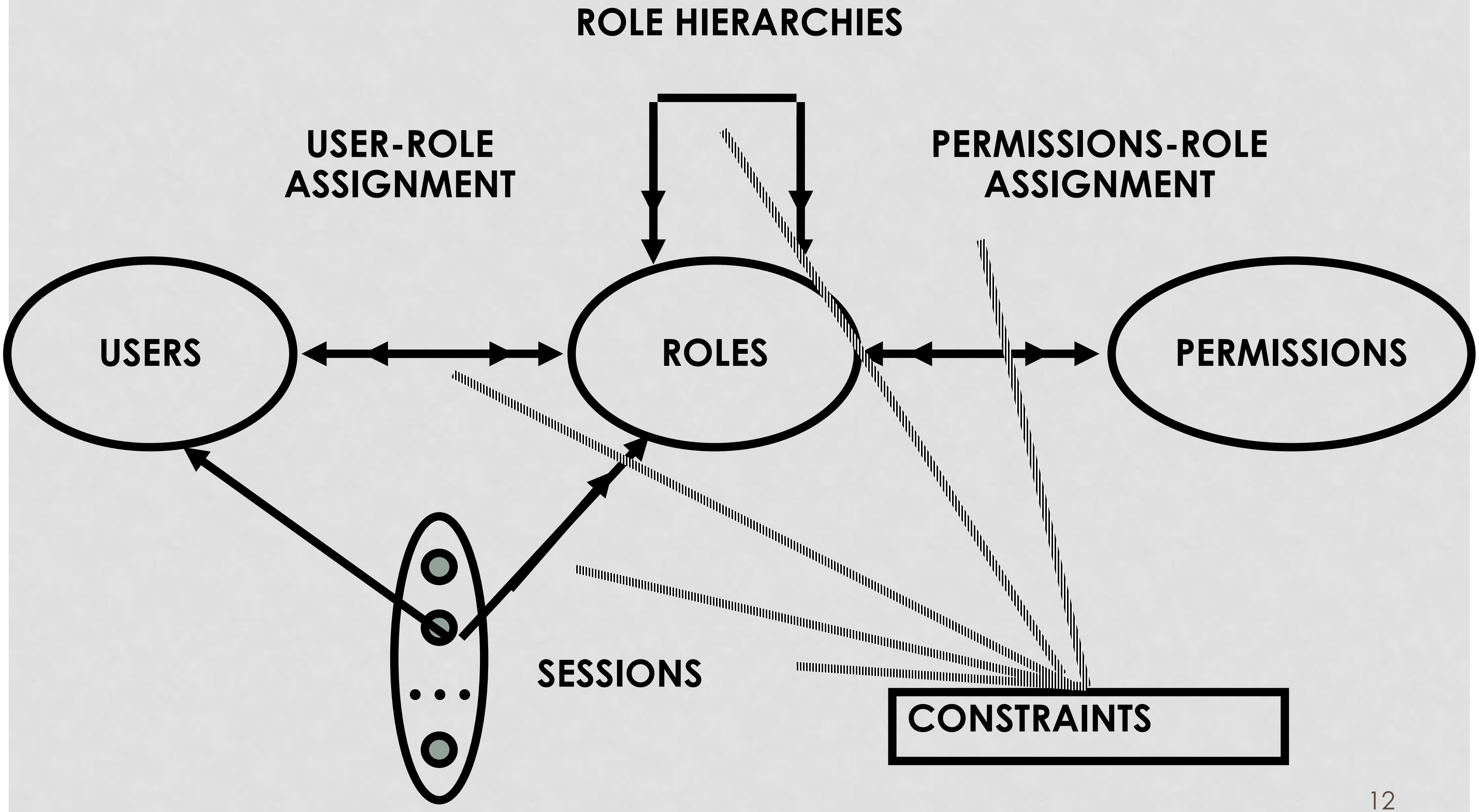
Physician

Health-Care Provider

RBAC2 (With Constraints)

- Example constraints
  - Mutual exclusion
  - Pre-condition: Must satisfy some condition to be member of some role
    - E.g., a user must be an undergrad student before being assigned the UTA role

RBAC2 (With Constraints)



Products Using RBAC

- Data Base Management Systems (DBMS)
- Enterprise Security Management
  - IBM Identity Manager

Next Lecture

- Web Security
- Readings for next lecture:
  - “Securing Your Web Browser” – US-CERT article.
    - us-cert.gov/publications/securing-your-web-browser
  - OWASP top 10.