IT2775 Operations Security

User Account Management

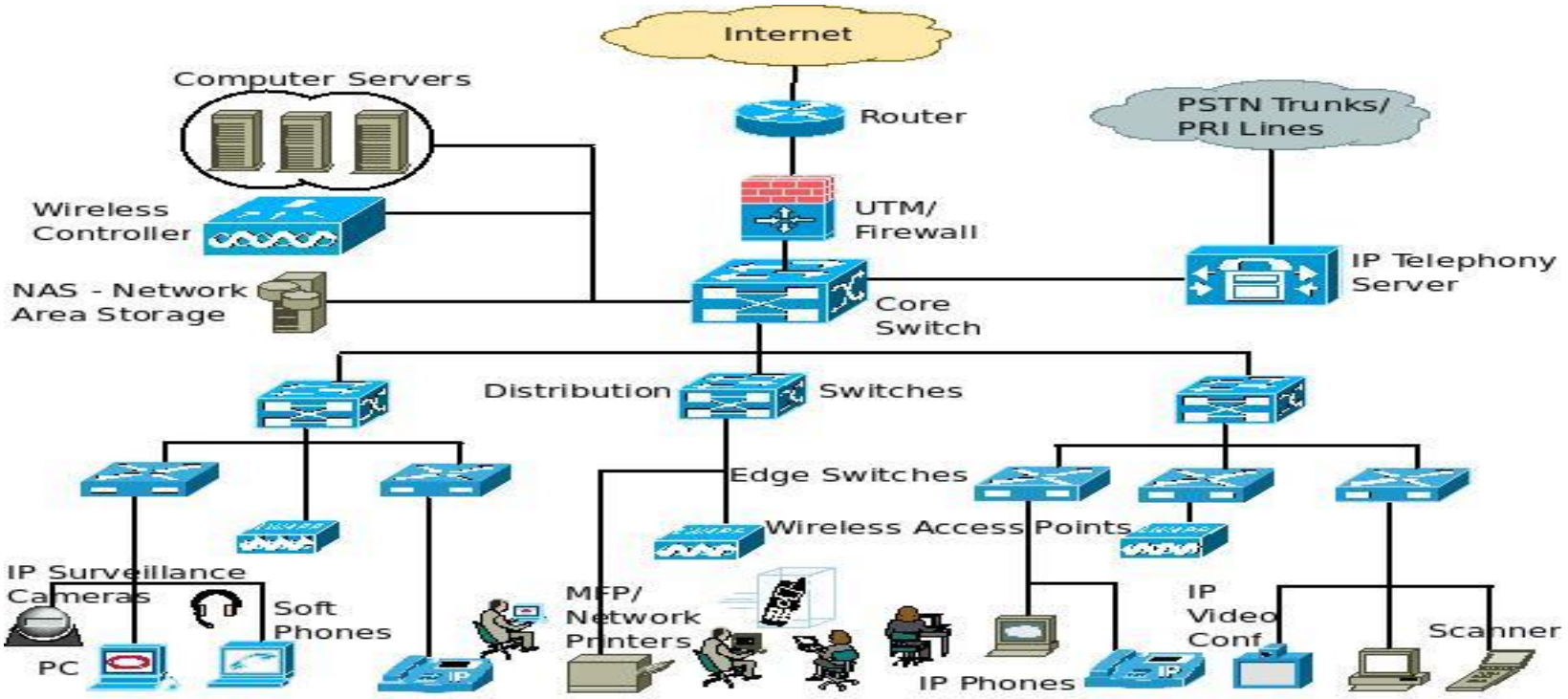
NANYANG POLYTECHNIC

Objectives

- Key principles of access control
- RBAC types (4)
- Visualise access rights
  - ACMs, ACLs
- Account types (2)
- User types (5)
- Others
  - Temporal Access Control
  - Clearance
  - Account Validation

What is Access Control?

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.



Key Principles for Access Control

- Need-to-know
  - Assign access only when there is a need to. User may still be denied access even if clearance is given.
- Least privileges
  - Assign minimum rights/access to specific objects in order to perform a task.

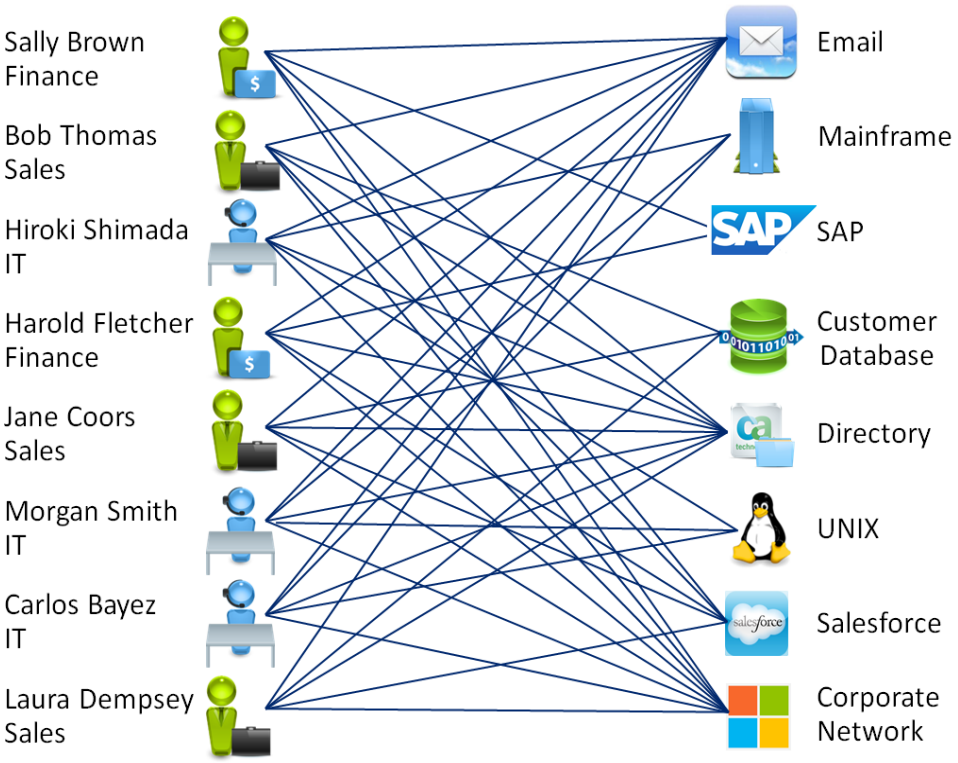
- Separation of duties
  - Restrict privileges of any one user so that more than one user is required to complete an important task.

RBAC

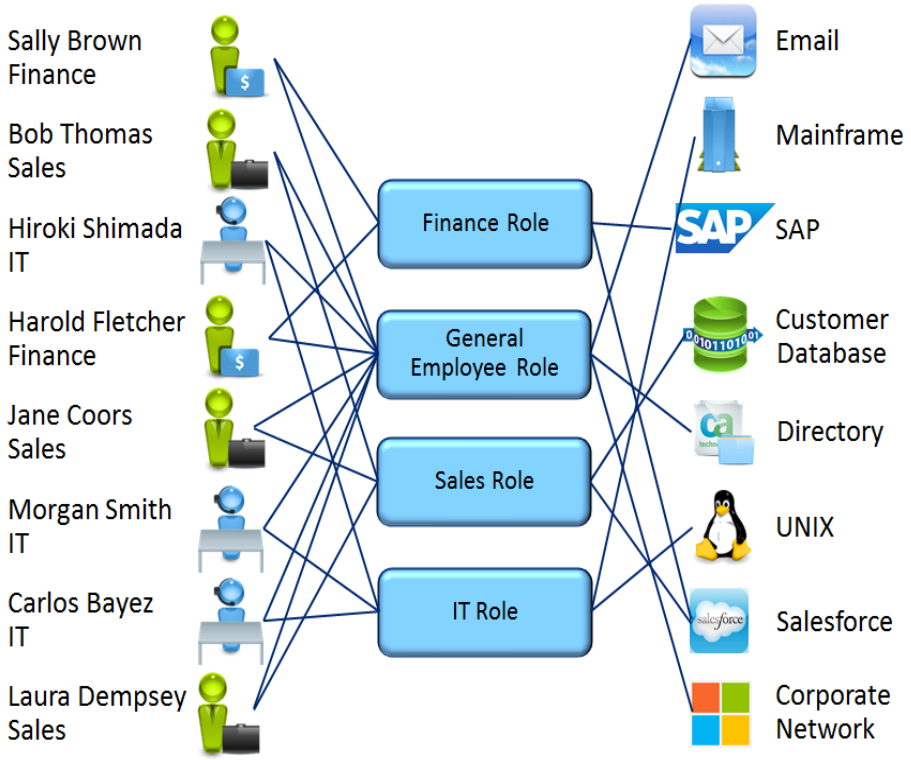
- Role Based Access Control(RBAC):
  - An approach to restricting system access to authorized users.
  - Allows for easy and effective management of privileges for a large number (> 500) of users.
  - Users => Roles => Permissions
- Key feature: All access is through roles.
- Widely accepted as best practice.
  - Microsoft Active Directory, FreeBSD SELinux. SQL Server, Solaris, Oracle, PostgreSQL, SAP and major Identity Management software vendors.

RBAC

w/o roles



with roles



Extracted from https://wiki.ca.com/display/GM12602/Access+Governance+and+RBAC

RBAC History

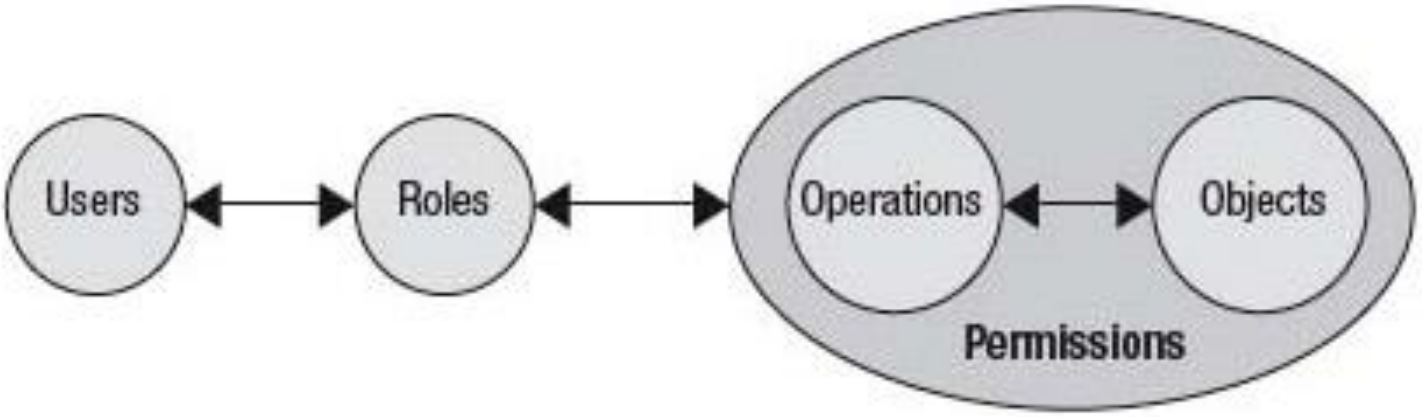
- 1992: Formal model of RBAC (Ferraiolo, Kuhn)
- 1996: Family of RBAC models (Sandhu et al.)
- 2000: Unified RBAC model as a proposed standard (Sandhu, Ferraiolo, Kuhn)
- 2004: RBAC model became ANSI standard
- 2010: Adding attributes to RBAC (Kuhn et al.)

RBAC Types

- Four main types of RBAC
  1. Flat RBAC (Basic RBAC)
  2. Hierarchical RBAC (Flat RBAC + Inheritance)
  3. Constrained RBAC (Hierarchical RBAC + SOD)
  4. Symmetric RBAC (Constrained RBAC + Role Review)

1. Flat RBAC

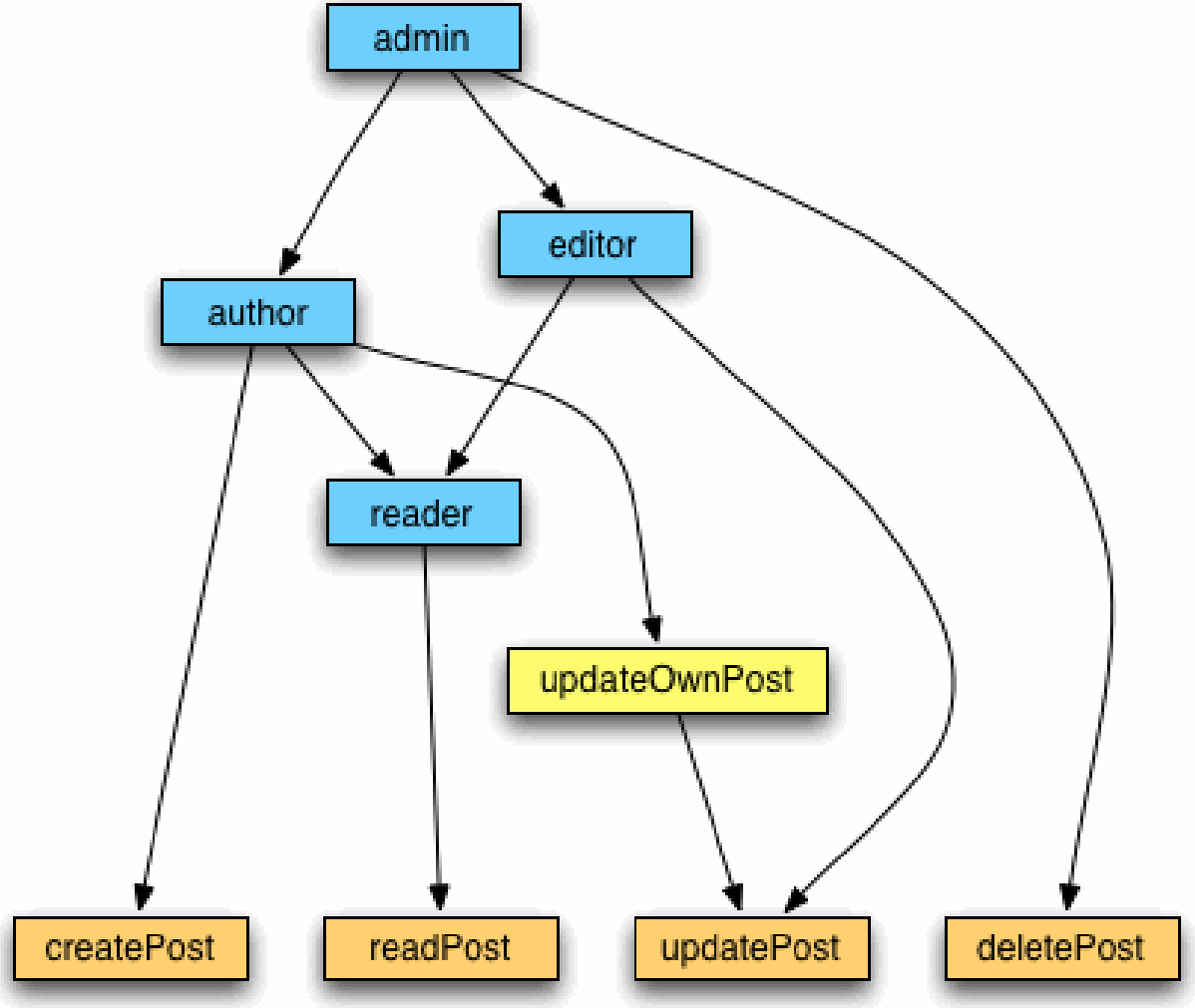
- Simple user-role-permission relationship.
- Many-to-many user-role assignment and permission-role assignment relation.
- ✘ No limit on the no. of roles a user can have
- ✘ No restriction to activate one role at a time.



2. Hierarchical RBAC

- Flat RBAC plus …
  - simple role hierarchy relations among roles
  - means to reflect lines of authority in organizations
- Inheritance and activation hierarchies
  - Inheritance (all): When parent is activated, all permissions assigned to child are also activated.
  - Activation (partial): When parent is activated, need to select which child's permissions to be activated. May restrict only 1 child's permissions be activated.
  - ✘ Tend to concentrate permissions to parent nodes, creating roles with many permissions.

Hierarchical RBAC Example



3. Constrained RBAC

- Hierarchical RBAC plus …
  - Further restrictions on the hierarchy feature – Separation of Duties (SOD).
  - 2 types of SOD
    - Static SOD (design time) – identify relationships between conflicting roles and restrict users from being assigned to these roles at the same time.
    - Dynamic SOD (run time) – identify relationships that conflict when acted upon at the same time and users can be assigned to these roles, but cannot activate both roles at the same time.

Separation of Duties

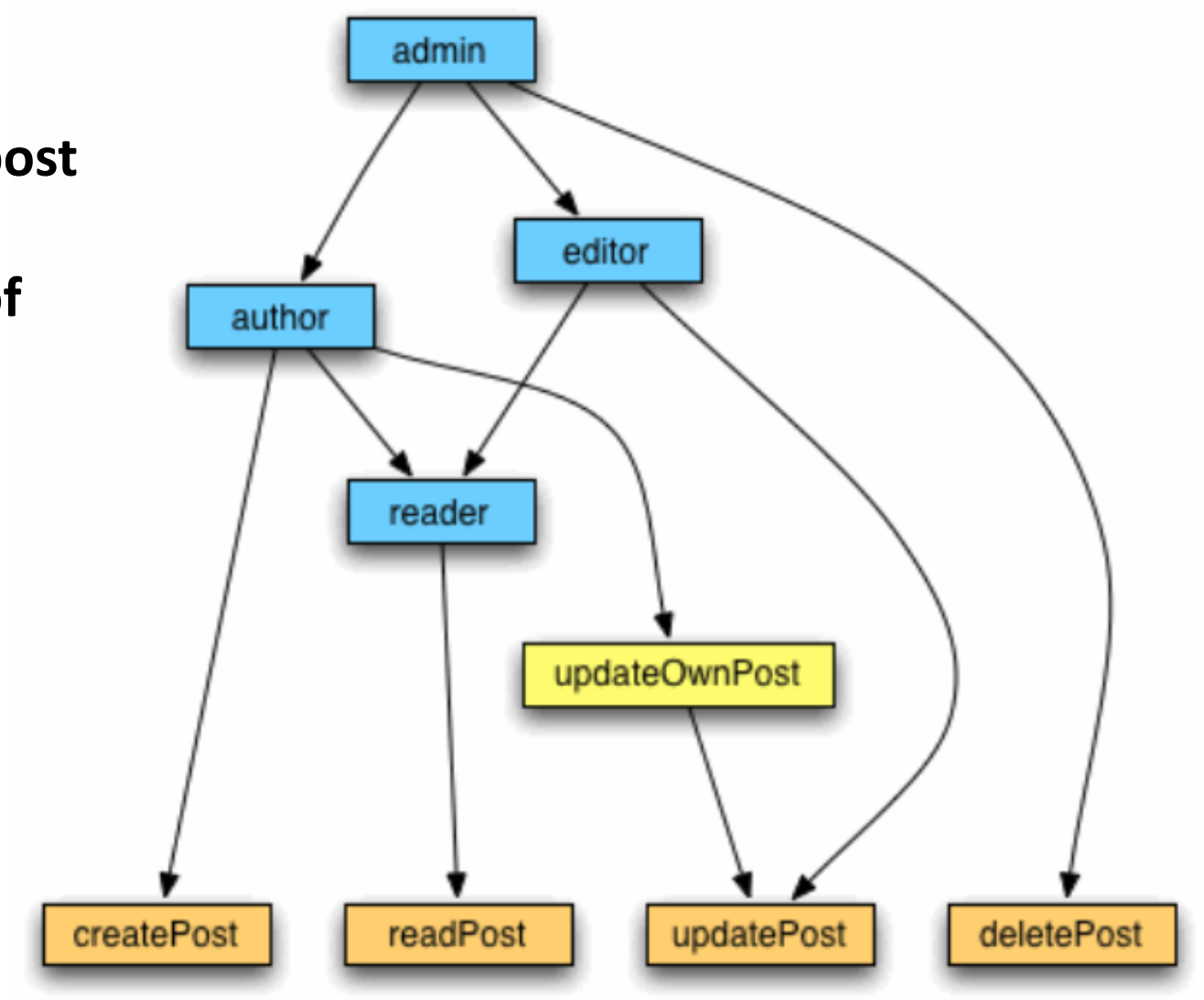
- Avoid conflict of interest
- Check and balance
- Ensure 2 or more people must be involved in authorizing critical operations

Example:

- Purchaser cannot be same person as approver
- Policeman cannot be same as judge

Dynamic SOD

Author can update own post but cannot update post of others.

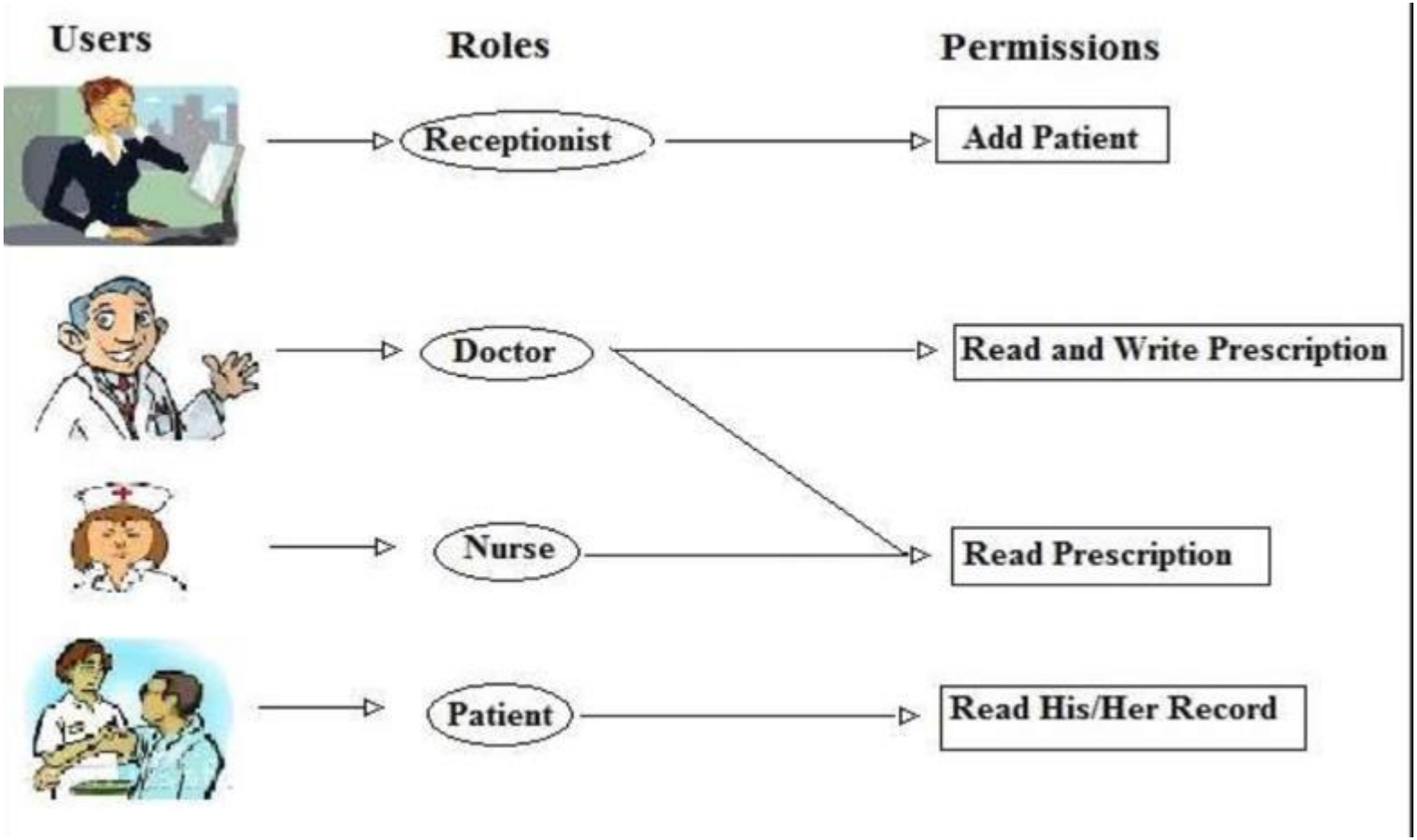


4. Symmetric RBAC

- Constrained RBAC plus …
  - Permission-role review to maintain permission assignments (user resigned, changed roles).
    - complete set of objects associated with the permissions assigned to a particular user/role.
    - complete set of operation-object pairs associated with the permissions assigned to a particular user/ role.
  - Maintains quality of the authorisation database.

Other forms of Access Control

RBAC


Users
Roles
Permissions
Receptionist
Add Patient
Doctor
Read and Write Prescription
Nurse
Read Prescription
Patient
Read His/Her Record

Visualising Access Rights

- Visual Mechanisms
  - Shows permission assignment to roles, roles to users.
  - Reflects the actual implementation visually.
  - Help see user-role-permission relationships.

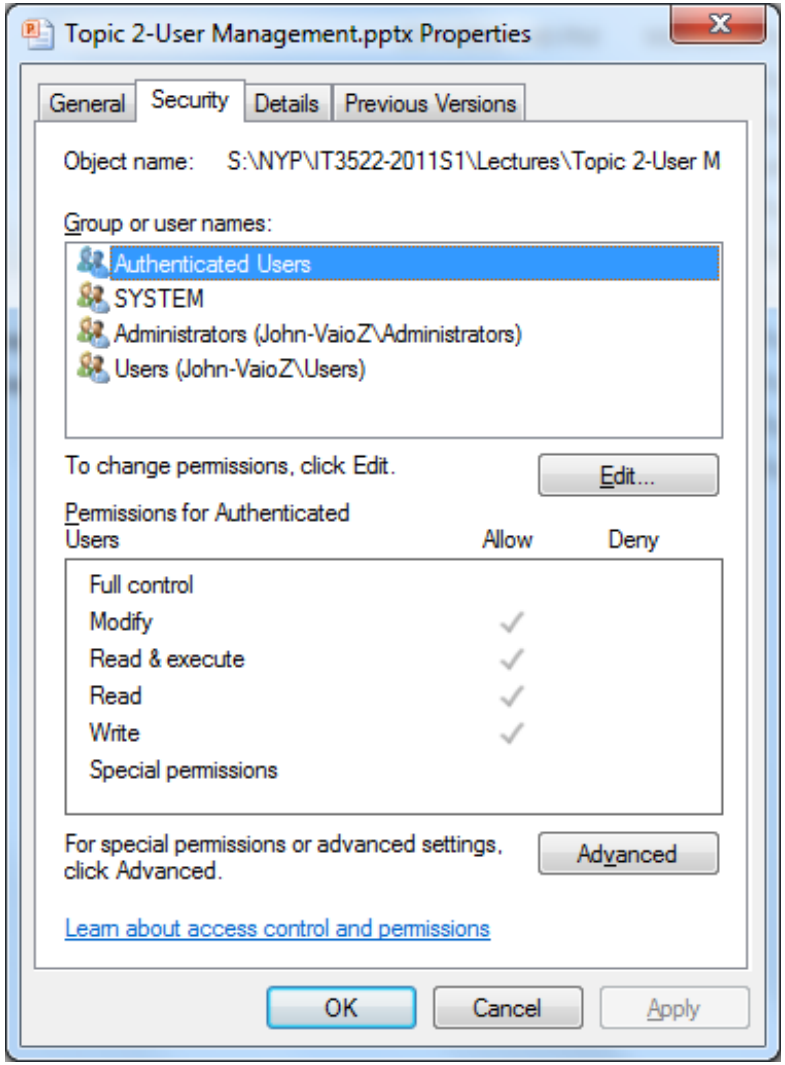
1. Access Control Matrix
   - Table of permissions vs. groups (roles) and/or users.
2. Access Control List
   - list of permissions assigned to groups (roles) and/or users.

Visualising Access Rights

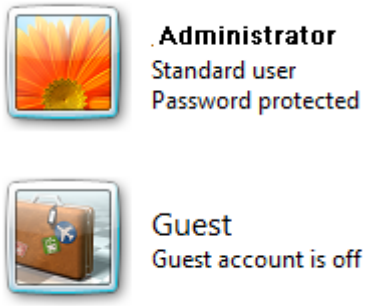
	R_1	R_2	...	R_n
U_1	✕			
U_2	✕			
U_3		✕		✕
U_4				✕
U_5				✕
U_6				✕
...				
U_m	✕			

OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_2	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
...									
R_n			control		write	stop			



Accounts and Users



- User Accounts
  - Privileged
    1. Built in admin
    2. Admin
    3. Service
  - Non-Privileged
    1. User

- User Types
  1. System admin
  2. Operators
  3. Security admin
  4. Helpdesk personnel
  5. End users

User Accounts

1. Built-in administrator (root) accounts
   - All-powerful default administrator account.
   - Generally shared by administrators to perform specialized administrative tasks.
     - When shared, electronic logs should be activated to track individual use of the root account.
     - Manual logs may also be kept and checked for consistency with the electronic logs.
   - For all other tasks, should use individual administrator accounts.
   - Remote login using root accounts should be disabled, and encrypted if absolutely required.

User Accounts

2. Administrator accounts
   - Accounts for individual administrators to perform common administrator/maintenance tasks.
     - Distributed in person and documented in writing. Need to sign undertaking to use follow usage policies.
     - Removed immediately after administrator has left.
     - Revalidate business needs for the account regularly.
   - Utilize external logging mechanisms as administrators may be able to tamper with the built-in logging mechanisms.

User Accounts

3. Service accounts
   - Privileged access by system services and applications such as web servers, email servers, DBMS.
     - Some services, such as Oracle, create multiple accounts at initial installation.
   - Passwords for service accounts should be complex and/or restricted only to the particular program.
     - E.g. Quarterly password change. 
   - Past malware incidents took advantage of default service accounts to install rootkits or backdoors.
4. User
   - Most users are assigned ordinary accounts.

User Types

1. System Administrators
   - Typically assigned the highest privileges.
   - Perform key administration/maintenance tasks.
   - Used by trained and authorized individuals.
2. Operators
   - Provide day-to-day operations in a data centre.
     - Higher privileges than users but lower than administrators.
     - E.g. load programs, monitor events in the system, mount volumes, control job flows, change configurations, manipulate I/O devices.

User Types

3. Security Administrators
   - Oversees security operations in systems.
     - E.g. account management, assignment of file security labels, system security settings.
   - Typically lower privileges than System Admin.
     - Separate Security Admin and System Admin for check and balance.
4. Helpdesk Personnel
   - Privileges to provide front line support to users
     - E.g. unlocking accounts, resetting passwords.
5. End Users
   - Regular staff requiring access to IT resources.

Temporal* Access Control

- Need for temporary access control
  - E.g. Auditing by 3rd parties, external contractor performing a task, staff covering duties.
- Problem: removing the access when not needed, in a timely manner.
- Systems today provide pre-setting (template) of window-of-access to ensure temporary access is removed when not needed.

*Temporal: Relating to time or limited by time

Clearance

- Conducted prior to providing account to user.
- Granted to individuals according to
  - their trustworthiness
    - E.g. Whether the user has demonstrated a serious lack of judgement or illegal activity
    - E.g. Clearance interview 
  - the level of access to sensitive information needed
- Helps to measure the likelihood of a person's compliance with organizational policy.

Account Validation

- Active accounts: remain enabled
- Inactive accounts: likely to be disabled
  - Periodic reviews of accounts for inactivity.
  - Verify reasons for inactivity
    - Extended leave, resignations: should be disabled

Summary

- Key principles of access control
- RBAC types (4)
- Visualise access rights
  - ACMs, ACLs
- Account types (2)
- User types (5)
- Others
  - Temporal Access Control
  - Clearance
  - Account Validation