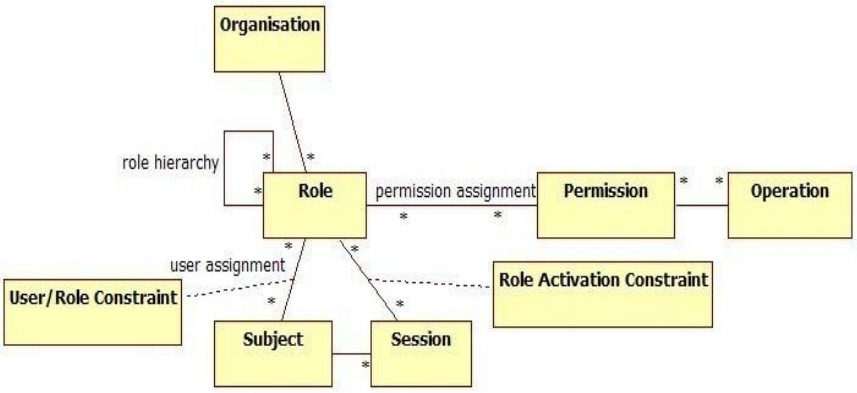
Role Based Access Control (RBAC)

The earliest forms of access control systemsassigned privileges to users. These early access control systems allowed the system administrator to enable defined privileges for users like *Bob* and*Doug*.
The addition of user groups improved that situation. The system administrator could now assign privileges to groups such as *Sales* or*Accounting* and add users into those groups.
Role Based Access Control (RBAC) is the next evolutionary step in access control.
Role Based Access Control (RBAC) enables privileges to be assigned to arbitrary roles. Those roles can then be assigned to real users.

The provides more granular control of privileges, which enhances system security. In addition, it reduces the amount of administrative effort required to add or delete system users.

Role Based Access Control (RBAC) under Solaris



Sun Microsystems added support for Role Based Access Control (RBAC) in Solaris 8. The Solaris Role Based Access Control (RBAC) system is an excellent model to study in order to understand Role Based Access Control (RBAC) systems in general.

The building blocks of Solaris Role Based Access Control (RBAC) are Authorizations and Privileged Operations. Profiles are built from these two building blocks. These Profiles may then be added to Roles.

Authorizations

Authorizations are rights to perform specifically defined administration functions. Authorizations are defined in the auth_attr file.
The `auths` command is used to print the authorizations granted to a user.

```
# auths will

solaris.audit.read
```

Privileged Operations

Privileged Operations are rights to execute specifically defined Solaris commands. Privileged Operations are defined in the exec_attr file.

Profiles

Groups of Authorizations and Privileged Operations are known as Profiles. Profiles are defined in theprof_attr file.
The `profiles` command is used to print the profiles defined for a user.

```
# profiles will

Audit Management, All Commands
```

user_attr and policy.conf

Authorization, Profile, and Role assignments are stored in the user_attr file. Authorization and Profile assignments for all users on the system are stored in the policy.conf file.

Roles

Roles are special system accounts. Roles are similar to regular system users, however roles may not log into the system. The preferred method of assuming a role is to use the `su` command.

The `roles` command is used to print the roles defined for a user.

```
# roles will

admin
```

Roles are added, modified, and deleted using the `roleadd`, `rolemod` and `roledel` commands.

Source: http://www.tech-faq.com/role-based-access-control-rbac.html