Deadlock

Occurs when user program compete for resources

Harware

files

sychronization primitives

Thread A Thread B

lockA-> Acquire LockB ->Acquire

| |

| |

lockB->Acquire LockA->Acquire

two or more jobs are each waiting on an event that can only be generated by one of the waiting jobs

Using Resource Sequence

a->User program requests resource from os

b->once access granted, resource is used

c->resource given back to O.S.

What if a requested resource is not available?

a->Fail the request

+Deadlock not possible

-Not nice to user programs

b->Queue the request

-Deadlock can occur

+Easy on userprogram

4 conditions for Deadlock ( need all 4 to produce Deadlock)

a->Mutual Exclusion

Resources that can’t be shared

b-> Hold & Wait

I have resources. I hold onto them, ask for another resource & wait for it

c->No preemption

Some resources can not be “borrowed” & given back

d->circular Wait

Loop/cycle in resource allocation graph

J1 <

Request / \ Owns

/ \

\/

R2 R1

^

\ /

Owns \ / Request

> J2

Protection Systems

OS has this responsibility

General Characteristics

An OS has resources(objects)

that need protection

They are managed by the OS

For user programs

Each resource has a unique ID

Each resource has a valid set of operations that can be performed

Protection Systems have 3 components

Resource to be protected

A set of allowed operations

Processes

Domain Matrix Implementation

Use a 2D array

Domain: A set of pairs of protection data

resources/objects

rights(authorized operations)

Rules:

A user can only belong to 1 domain@a time

“ “ “ “ switch domains

Each object/rights pair specifies

Object being protected

subset of operations your domain are allowed to perform

In our matrix

A row represents a domain

A column represents an object

A cell contains the rights for a domain for an object

Example: aludra

#users: 10,000 domains

#files: 1,000,000

10,000,000,000 cells

10,000,000 in use

Two “standard” implementations

Rule: Only store data for what a user program can access

no data means no access

a->Access Control List(ACL)

by resource

List of pairs: domain & rights

b-> Protection Domain

By domain

Protection data is privileged

At any point in time, the protection data establishes what a domain can access

|

|

\/

It does not control what you are authorized to do

|

|

\/

Policy v.s. Mechanism

3 levels 7 0 0

world R W X

group 1 1 1

domain 7 7 7

Scenario

New computer - no users yet

There is data to be protected

The authorization policies are implemented exactly

we have trustworthy people for above

Question: Can we guarantee the protection data will always match the policy?

No - By example

Tax Program:

computes taxes

No I/O except w/ user

No network sniffing possible

There is a “collaborator” w/ access to the server

is a programmer on tax s/w

two was to “share” w/ other user on the server

Pagefaults

⇒ I affect system performance

CPU usage

every 5 econds

pagefault rate above

above some level => 1 bit

below level => 0 bit

(this is still transferring some information, the change rate)