امیر محمّد آقاپور ۹۶۳۱۰۰۸ تمرین ۳

۱.

الف)

سیستم چند هسته ای: بین همه یک سیستم عامل اجرا می شود و مدیریت می کند، نحوه ارتباط به صورت tightly coupled است یعنی ارتباط روی برد و حتی در چند هسته ای داخل تراشه است، پردازنده ها روی کار هم نظارت نمی کنند و اطمینان پذیری کم است، سیستم عامل خود می تواند برنامه در حال اجرا را بین پردازنده ها تقسیم کند، محل ذخیره سازی و دیگر منابع مشترک توسط سیستم عامل مدیریت می شود.

سیستم خوشه ای: هر نود یک سیستم است و سیستم عامل جدا اجرا می کند، ارتباط به صورت loosely coupled است یعنی با استفاده از ارتباط شبکه ای مثل LAN یا WAN، بدلیل وجود هاست های جدا قابل اعتماد است و در صورت شکست(fail) یکی نود ناظر می تواند کار را به عهده بگیرد، برای کار های نیاز به کارایی بالا برنامه باید موازی سازی شود، نیاز به برنامه جدا برای مدیریت محل ذخیره سازی مشترک بین نود ها هست زیرا بیشتر سیستم عامل ها این کار را نمی توانند انجام دهند.

ب)

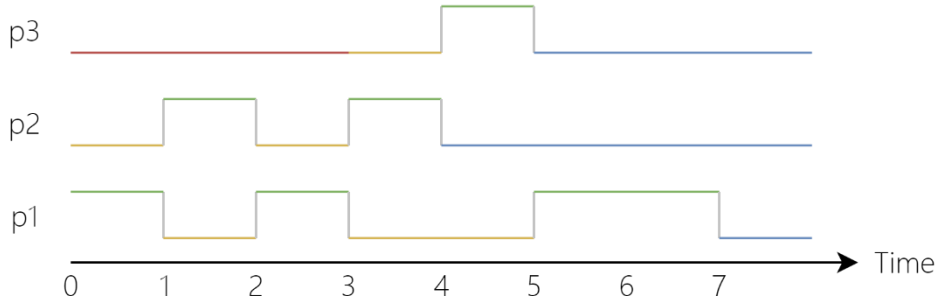
استفاده از سیستم مدیریت قفل توزیع شده(DLM): نقاط قوت: هر نود دسترسی کامل به پایگاه داده را دارد، داده اضافه(Redundancy) کم است. نقاط ضعف: برای تعداد نود بالا کارا نیست، قابل اعتماد(Reliable) نیست.

استفاده از شبکه محلی محل ذخیره سازی(SAN): نقاط قوت: قابل استفاده برای سیستم های خوشه ای بزرگ(آن ها که با WAN متصل شده اند به طور مثال)، قابل اعتماد بودن بدلیل وجود نسخه های مختلف در هاست های دیگر که در صورت شکست یکی میتوان از دیگری استفاده کرد. نقاط ضعف: وجود داده اضافه، سرعت پایین تر

۲.

فرض کنیم ابتدا یک برنامه(process) دارای رابط کاربری(GUI) اجرا می شود و یک برنامه برای خواندن از فایل و انجام محاسباتی روی آن را اجرا می کند. در multiprogramming وقتی برنامه دوم منتظر خوانده شدن از فایل است(I/O operation)، پردازنده به اجرای برنامه قبلی، یعنی رابط کاربری می پردازد و رابط پاسخگو(responsive) می شود و می توان با آن کار کرد ولی بعد از اتمام کار خوانده شدن از فایل، دیگر این طور نخواهد بود و تا پایان محاسبات روی داده های خوانده شده، با رابط کاربردی نمی توان کار کرد. در time sharing امّا پردازنده در تمام زمان ها حتی بعد از اتمام خوانده شدن فایل، در فاصله زمانی های کوتاه، بین این دو برنامه جابجایی(switch) انجام می دهد و رابط کاربری همیشه پاسخگو خواهد بود.

۳.



رنگ سبز یعنی در حال اجرا، زرد یعنی منتظر سهم زمانی، قرمز یعنی هنوز وارد نشده و آبی یعنی تمام شده است.

$$\text{Average Response Time} = \frac{2+4+7}{3} = 4.3 \text{ s}$$

لازم به ذکر است زمان پاسخگویی، مدّت زمان از ورود(آماده به اجرا شدن) برنامه تا اتمام کار آن در نظر گرفته شده و بین سه برنامه میانگین محاسبه شده است.

.۴

الف) برای تمییز دادن دستورات از طرف برنامه کاربر از دستورات از طرف سیستم عامل توسط پردازنده و کنترل دسترسی های آن ها طوری که برنامه کاربر نتواند کار های حساس را انجام دهد. در این صورت برنامه های غیر صحیح و نا امن و مخرب نمی توانند باعث ایجاد خرابی در کل سیستم شوند. پس در کل برای تأمین صحیح کار کردن و امنیّت سیستم لازم است به صورت سخت افزاری این کنترل ها اعمال شود.

ب) دستورات حساسی که ممکن است در صورت اجرای نا بجا و نادرست باعث صدمه و خرابی سیستم شوند؛ مانند کنترل I/O، مدیریّت تایمر، مدیریّت وقفه ها. این دستورات باید توسط سیستم عامل انجام شوند و برنامه کاربر در صورت نیاز باید system call انجام دهد.

ج) برای درایور های دستگاه های جانبی(device drivers) یا برنامه ماشین مجازی(virtual machine) زیرا دسترسی های بیشتری از کاربر نیاز دارد ولی دسترسی کامل بهتر است نداشته باشد.

.۵

حفاظت(Protection)	**امنیّت**(Security)	**مفهوم**
استفاده بدون اجازه و مخربانه منابع توسط استفاده کننده های فاقد صلاحیت - ارور در رابط ها(interface) که باعث مشکل در زیر سیستم ها می شود	حملات داخلی و خارجی مانند ویروس ها و محروم سازی از سرویس و یا دزدیده شدن اطلاعات کاربر و استفاده مجاز امّا غیر قانونی از سیستم	**نوع تهدید هایی که سیستم درگیر آن است**
منابع سیستم	دسترسی و تغییر داده های موجود در سیستم و یا ایجاد تغییر در خود سیستم	**نوع درخواست هایی که مدیریّت شده**
فقط استفاده کننده های مجاز اجازه دسترسی به منابع را داشته باشند	تشخیص استفاده کننده قانونی و محافظت از داده های دیگر کاربران در برابر حملات	**سیاست**
روش هایی برای ایجاد و اطمینان از رعایت شدن قوانین برای دسترسی مجاز	دسته بندی کاربران و استفاده از شناساگر امیتی(SID) برای نظارت و مدیریت دسترسی ها، تشخیص دسترسی های غیر قانونی و مخرب	**مکانیزم**

.۶

۱: شبکه وسیع(جهانی) Wide Area Network

۲: شبکه شهری Metropolitan Area Network

۳: شبکه محلّی Local Area Network

۴: شبکه شخصی Personal Area Network

۷.

الف) نادرست. شبیه سازی سیستم عامل وابسته به نرم افزار بر روی سیستم عامل وابسته به سخت افزار را مجازی سازی گویند.

ب) نادرست. عمل تقلید داخل سیستم عامل دیگر انجام نمی شود و باید دستورات دقیقاً مشابه سیستم اصلی مورد تقلید اجرا شوند.