Operating Systems

Lecture # 3

Department of Computer

4th Class

System Calls and Memory protection

By

Dr. Ahmed Khudhair Abbas

Computer and Internet Center

استدعاءات النظام في نظام التشغيل System Calls in Operating System

استدعاء النظام هو وسيلة لبرنامج مستخدم للتفاعل مع نظام التشغيل. يطلب البرنامج العديد من الخدمات ويستجيب نظام التشغيل من خلال استدعاء سلسلة من استدعاءات النظام لتلبية الطلب ويمكن كتابة استدعاء النظام بلغة التجميع أو لغة عالية المستوى مثل C أو Pascal. استدعاءات النظام هي وظائف محددة مسبقًا قد يستدعيها نظام التشغيل مباشرةً إذا تم استخدام لغة عالية المستوى.

ما هو استدعاء النظام What is a System Call

استدعاء النظام هو طريقة لبرنامج الكمبيوتر لطلب خدمة من نواة نظام التشغيل Kernel التي تعمل عليها استدعاء النظام هو طريقة للتفاعل مع نظام التشغيل عبر البرامج. بمعنى ان استدعاء النظام هو طلب من برنامج الكمبيوتر إلى نواة نظام التشغيل.

تعمل واجهة برمجة التطبيقات Application Program Interface (API) على توصيل وظائف نظام التشغيل ببرامج المستخدم ويعمل كحلقة وصل بين نظام التشغيل والعملية مما يسمح للبرامج على مستوى المستخدم بطلب خدمات نظام التشغيل ولا يمكن الوصول إلى نظام kernel إلا باستخدام استدعاءات النظام واستدعاءات النظام مطلوبة لأية برامج تستخدم الموارد.

كيف يتم إجراء استدعاءات النظام How are system calls made

عندما يحتاج برنامج الكمبيوتر إلى الوصول إلى نواة نظام التشغيل فإنه يقوم بإجراء استدعاء للنظام ويستخدم استدعاء النظام API لعرض خدمات نظام التشغيل لبرامج المستخدم وهي الطريقة الوحيدة للوصول إلى نظام النواة ويجب أن تستخدم جميع البرامج أو العمليات التي تتطلب موارد للتنفيذ استدعاءات النظام لأنها تعمل كواجهة بين نظام التشغيل وبرامج المستخدم.

فيما يلي بعض الأمثلة على كيفية اختلاف استدعاء النظام من وظيفة المستخدم system call varies from a user function

1. قد تقوم وظيفة استدعاء النظام بإنشاء واستخدام عمليات kernel لتنفيذ المعالجة غير المتزامنة.
2. استدعاء النظام له سلطة أكبر من روتين فرعي قياسي. يتم تنفيذ استدعاء نظام بامتياز وضع kernel في مجال حماية kernel.
3. لا يُسمح لاستدعاءات النظام باستخدام المكتبات المشتركة أو أي برامج غير موجودة في مجال حماية.kernel
4. يتم تخزين برامج وبيانات استدعاءات النظام في ذاكرة kernel

لماذا تحتاج إلى استدعاءات النظام في نظام التشغيل ?Why do you need system calls in Operating System

1. يجب أن يطلب عندما يريد نظام الملفات إنشاء أو حذف ملف.
2. تتطلب اتصالات الشبكة استدعاءات النظام لإرسال واستقبال حزم البيانات.

3. قراءة ملف أو كتابته بحاجة إلى استدعاءات النظام.
4. الوصول إلى الأجهزة ، بما في ذلك الطابعة والماسح الضوئي بحاجة إلى استدعاءات نظام.
5. يتم استخدام استدعاءات النظام لإنشاء وإدارة عمليات جديدة.

كيف تعمل مكالمات النظام How System Calls Work

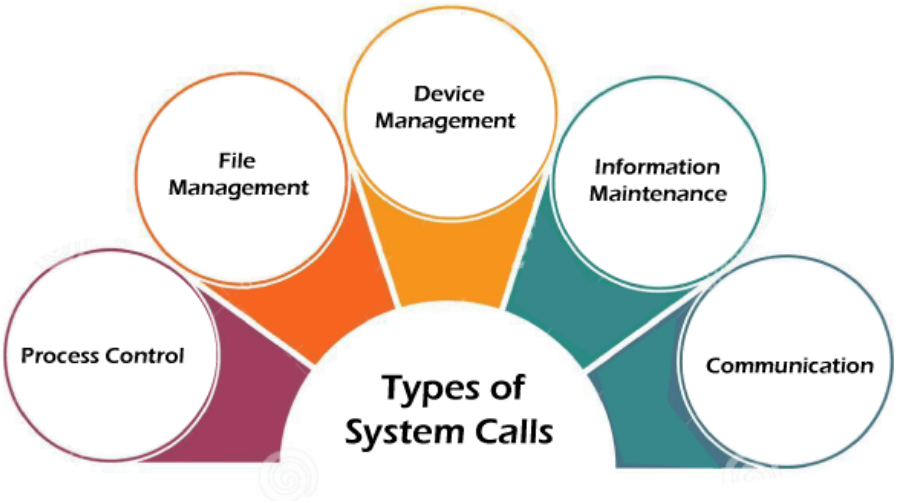
تعمل التطبيقات في منطقة من الذاكرة تُعرف باسم مساحة المستخدم User Space يتصل استدعاء النظام بنواة نظام التشغيل والتي يتم تنفيذها في مساحة kernel عندما يقوم أحد التطبيقات بإنشاء استدعاء نظام فيجب أولاً الحصول على إذن من ال kernel ويحقق ذلك باستخدام طلب مقاطعة والذي يوقف العملية الحالية مؤقتًا وينقل التحكم إلى ال.kernel

قد يستغرق استدعاء النظام البسيطة بضع من النانو ثانية لتقديم النتيجة مثل استرداد تاريخ النظام ووقته وقد تستغرق مكالمة النظام الأكثر تعقيدًا مثل الاتصال بجهاز الشبكة بضع ثوانٍ وتطلق معظم أنظمة التشغيل مؤشر ترابط kernel مميز لكل استدعاء للنظام لتجنب الاختناقات. أنظمة التشغيل الحديثة متعددة الخيوط مما يعني أنها تستطيع التعامل مع مكالمات النظام المختلفة في نفس الوقت.

أنواع مكالمات النظام Types of System Calls

هناك خمسة أنواع شائعة من مكالمات النظام:

1. **التحكم في العمليات Process Control**: التحكم في العملية هو استدعاء النظام المستخدم لتوجيه العمليات. تتضمن بعض أمثلة التحكم في العملية الإنشاء ، التحميل ، الإحباط ، الإنهاء ، التنفيذ ، المعالجة ، إنهاء العملية ، إلخ.
2. **إدارة الملفات File Management :** إدارة الملفات هي استدعاء نظام يتم استخدامه للتعامل مع الملفات. تتضمن بعض أمثلة إدارة الملفات إنشاء الملفات وحذفها وفتحها وإغلاقها وقراءتها وكتابتها وما إلى ذلك.
3. **إدارة الجهاز Device Management :** إدارة الجهاز هي مكالمة نظام تُستخدم للتعامل مع الأجهزة. تتضمن بعض أمثلة إدارة الجهاز القراءة ، والجهاز ، والكتابة ، والحصول على سمات الجهاز ، وإصدار الجهاز ، وما إلى ذلك.
4. **صيانة المعلومات Information Maintenance :** صيانة المعلومات هي استدعاء نظام يتم استخدامه للحفاظ على المعلومات. هناك بعض الأمثلة على صيانة المعلومات ، بما في ذلك الحصول على بيانات النظام ، وتعيين الوقت أو التاريخ
5. **الاتصالات Communication :** الاتصال هو مكالمة نظام يتم استخدامها للاتصال. هناك بعض الأمثلة على الاتصال ، بما في ذلك إنشاء اتصالات الاتصال وحذفها وإرسال الرسائل واستلامها وما إلى ذلك.



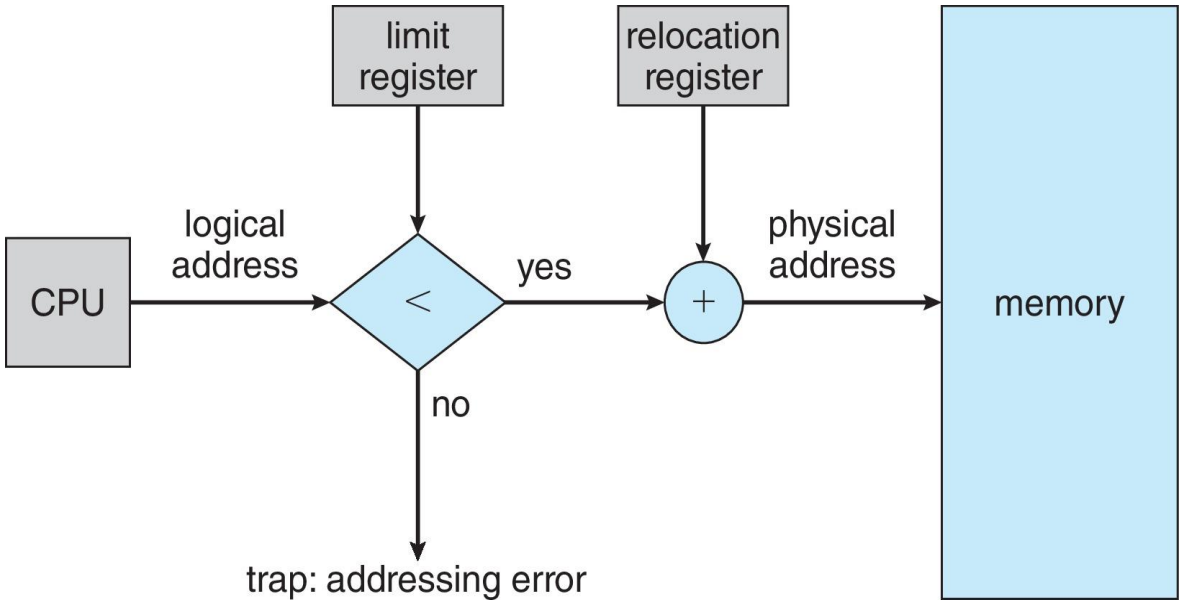
Examples of Windows and Unix system calls

There are various examples of Windows and Unix system calls. These are as listed below in the table:

Process	Windows	Unix
Process Control	CreateProcess() ExitProcess() WaitForSingleObject()	Fork() Exit() Wait()
File Manipulation	CreateFile() ReadFile() WriteFile() CloseHandle()	Open() Read() Write() Close()
Device Management	SetConsoleMode() ReadConsole() WriteConsole()	Ioctl() Read() Write()
Information Maintenance	GetCurrentProcessID() SetTimer() Sleep()	Getpid() Alarm() Sleep()
Communication	CreatePipe() CreateFileMapping() MapViewOfFile()	Pipe() Shmget() Mmap()

حماية الذاكرة في أنظمة التشغيل Memory Protection in Operating Systems

أن أنظمة التشغيل المختلفة تستخدم أشكالًا مختلفة من حماية أو فصل الذاكرة وفي حماية الذاكرة يتعين علينا حماية نظام التشغيل من عمليات المستخدم والتي يمكن القيام بها باستخدام relocation register بسجل حد limit register هنا يحتوي سجل relocation register على قيمة أصغر عنوان فعلي physical address بينما يحتوي limit register على نطاق العناوين المنطقية logical addresses هذان السجلان لهما بعض الشروط مثل كل عنوان منطقي يجب أن يكون أقل من limit register. وتُستخدم وحدة إدارة الذاكرة memory management unit لترجمة العنوان المنطقي logical address بالقيمة الموجودة في relocation register ديناميكيًا وبعد ذلك يتم إرسال العنوان المترجم (أو المعين) إلى الذاكرة.



Support for relocation and limit registers in process

في الرسم البياني أعلاه عندما يحدد المجدول scheduler عملية لعملية التنفيذ execution process ، يكون المرسل dispatcher من ناحية أخرى مسؤولاً عن تحميل سجلات relocation and limit registers بالقيم الصحيحة كجزء من تبديل السياق context switch مثل كل عنوان تم إنشاؤه بواسطة وحدة المعالجة المركزية CPU يتم فحصه مقابل هذين المسجلين ، وقد نحمي نظام التشغيل والبرامج وبيانات المستخدمين من التغيير من خلال هذه العملية قيد التشغيل.

الحاجة إلى حماية الذاكرة Need of Memory protection

تمنع حماية الذاكرة العملية من الوصول إلى الذاكرة غير المخصصة unallocated memory في نظام التشغيل لأنها تمنع البرنامج من السيطرة على مقدار زائد من الذاكرة وقد يتسبب في تلف يؤثر على البرامج الأخرى المستخدمة حاليًا أو قد يؤدي إلى فقدان البيانات المحفوظة. تساعد موارد حماية الذاكرة هذه أيضًا في اكتشاف التطبيقات الضارة malicious or harmful applications والتي قد تتلف بعد عمليات نظام التشغيل.

طرق حماية الذاكرة Methods of memory protection

هناك طرق مختلفة للحماية من الوصول إلى الذاكرة التي لم يتم تخصيصها وبعض الطرق شائعة الاستخدام مذكورة أدناه:

- **حماية الذاكرة باستخدام المفاتيح Memory Protection using Keys :**

يمكن العثور على مفهوم استخدام حماية الذاكرة مع المفاتيح في معظم أجهزة الكمبيوتر الحديثة بغرض تنظيم الذاكرة المقسمة إلى صفحات paged memory وللتوزيع الديناميكي بين برامج التشغيل المتوازية تعتمد المفاتيح على استخدام رموز خاصة حيث يمكننا التحقق من التوافق بين استخدام مصفوفات خلايا الذاكرة وعدد البرامج قيد التشغيل وتمنح هذه الطريقة الأساسية المستخدمين عملية لفرض الحماية على أساس الصفحة page-based protections دون أي تعديل في جداول الصفحات.

- **حماية الذاكرة باستخدام الحلقات Memory Protection using Rings :**

في علم الكمبيوتر تسمى المجالات domains المتعلقة بالحماية المطلوبة حلقات الحماية Protection Rings تساعد هذه الطريقة في تحسين التسامح مع الخطأ fault tolerance وتوفر الأمان. يتم ترتيب هذه الحلقات في تسلسل هرمي من الأكثر امتيازًا إلى الأقل امتيازًا most privileged to least privileged في نظام تشغيل المشاركة أحادي المستوى single-level sharing OS يحتوي كل جزء على حلقة حماية لعملية القراءة والكتابة وتنفيذ العمليات فإذا كان هناك استخدام لرقم حلقة أعلى من خلال العملية ، فإن رقم الحلقة الخاص بالمقطع يؤدي إلى حدوث خطأ لكن لدينا بعض الطرق لاستدعاء الإجراءات بأمان والتي يمكن تشغيلها برقم رنين أقل ثم العودة إلى رقم الحلقة الأعلى.

- **العنونة القائمة على القدرة Capability-based addressing :**

هي طريقة لحماية الذاكرة لا يمكن رؤيتها في أجهزة الكمبيوتر التجارية الحديثة. هنا يتم استعادة المؤشرات pointers (التي تتكون من عنوان ذاكرة) بواسطة كائنات القدرات capabilities objects التي لا يمكن إنشاؤها إلا من خلال التعليمات المحمية ويمكن تنفيذها فقط من خلال نواة Kernel أو من خلال عملية أخرى مصرح لها بالتنفيذ ، وبالتالي فهي تمنح ميزة للتحكم في العمليات غير المصرح بها في إنشاء مساحات عناوين منفصلة إضافية في الذاكرة.

- **حماية الذاكرة باستخدام الأقنعة Memory Protection using masks**

تستخدم الأقنعة في حماية الذاكرة أثناء تنظيم الصفحات organization of paging في هذه الطريقة ، قبل التنفيذ تتم الإشارة إلى أرقام الصفحات لكل برنامج ويتم حجزها لوضع توجيهاتها. هنا يتم منح الصفحات المخصصة للبرنامج الآن التحكم في نظام التشغيل في شكل رمز قناع (رمز ثنائي بت) والذي يتم تشكيله لكل برنامج عمل يتم تحديده بواسطة عدد البت

- **حماية الذاكرة باستخدام التجزئة Memory Protection using Segmentation**

هي طريقة لتقسيم ذاكرة النظام إلى أجزاء مختلفة. تُستخدم هياكل البيانات الخاصة بمعمارية x86 لنظام التشغيل مثل جدول واصف محلي local descriptor وجدول واصف عالمي global descriptor في حماية الذاكرة.

- **حماية الذاكرة باستخدام التجزئة المحاكاة Memory Protection using Simulated segmentation**

باستخدام هذه التقنية ، يمكننا مراقبة البرنامج لتفسير تعليمات كود الآلة الخاصة بهياكل النظام ويمكن للمحاكاة المساعدة في حماية الذاكرة باستخدام التجزئة باستخدام المخطط والتحقق من صحة العنوان الهدف لكل تعليمات في الوقت الفعلي.

حماية الأجهزة ونوع حماية الأجهزة Hardware Protection and Type of Hardware Protection

أن نظام الكمبيوتر يحتوي على الأجهزة مثل المعالج والشاشة وذاكرة الوصول العشوائي وغيرها الكثير ، وشيء واحد يضمنه نظام التشغيل أن هذه الأجهزة لا يمكن للمستخدم الوصول إليها مباشرة.

بشكل أساسي ، يتم تقسيم حماية الأجهزة إلى 3 فئات: حماية وحدة المعالجة المركزية وحماية الذاكرة وحماية الإدخال / الإخراج. على النحو التالي.

1. حماية وحدة المعالجة المركزية CPU Protection

يشار إلى حماية وحدة المعالجة المركزية لأننا لا نستطيع إعطاء وحدة المعالجة المركزية لعملية ما إلى الأبد ، يجب أن يكون ذلك لبعض الوقت المحدود وإلا فلن تحصل العمليات الأخرى على فرصة للتنفيذ. لذلك يتم استخدام عداد الوقت timer للخروج من هذا الموقف والذي يمنح بشكل أساسي قدرًا معينًا من الوقت للعملية وبعد تنفيذ الموقت ، سيتم إرسال إشارة إلى العملية لمغادرة وحدة المعالجة المركزية. ومن ثم لن تحتفظ العملية بوحدة المعالجة المركزية لمزيد من الوقت.

2. .2حماية الذاكرة Memory Protection

في حماية الذاكرة ، نتحدث عن هذا الموقف عندما تكون هناك عمليتان أو أكثر في الذاكرة وقد تصل إحدى العمليات إلى ذاكرة العملية الأخرى. ولمنع حدوث هذا الموقف ، نستخدم سجلين على النحو التالي:

1. **السجل القاعدة Base register**
2. **تسجيل الحد Limit register**

يقوم مسجل Base register بتخزين عنوان بدء البرنامج starting address وتخزين السجل الحد limit register لحجم العملية لذلك عندما تريد إحدى العمليات الوصول إلى الذاكرة ، يتم التحقق من إمكانية الوصول إلى الذاكرة أو عدم قدرتها على الوصول إليها.

حماية الإدخال / الإخراج I/O Protection

عندما نضمن حماية الإدخال / الإخراج I/O protection فلن تحدث بعض الحالات مطلقًا في النظام مثل:

1. إنهاء الإدخال / الإخراج لعملية أخرى Termination I/O of other process

2. عرض الإدخال / الإخراج لعملية أخرى View I/O of other process
3. إعطاء الأولوية لعملية إدخال / إخراج معينة Giving priority to a particular process I/O

حماية النظام في نظام التشغيل System Protection in Operating System

تشير الحماية إلى آلية تتحكم في وصول البرامج أو العمليات أو المستخدمين إلى الموارد المحددة بواسطة نظام الكمبيوتر. يمكننا أن نأخذ الحماية كمساعد لنظام تشغيل متعدد البرمجة multi programming بحيث يمكن للعديد من المستخدمين مشاركة مساحة اسم منطقي مشتركة بأمان مثل الدليل أو الملفات.

الحاجة للحماية Need of Protection

- لمنع وصول المستخدمين غير المصرح لهم
- للتأكد من أن كل برامج أو عمليات نشطة في النظام تستخدم الموارد فقط كما هو مذكور ،
- لتحسين الموثوقية من خلال الكشف عن الأخطاء الكامنة.

دور الحماية Role of Protection

يتمثل دور الحماية في توفير آلية لتنفيذ السياسات mechanism التي تحدد استخدامات الموارد في نظام الكمبيوتر ويتم تحديد بعض السياسات وقت تصميم النظام وبعضها تم تصميمه بواسطة إدارة النظام والبعض الآخر يتم تحديده بواسطة مستخدمي النظام لحماية ملفاتهم وبرامجهم.

يحتوي كل تطبيق على سياسات مختلفة لاستخدام الموارد وقد تتغير بمرور الوقت لذا فإن حماية النظام ليست فقط من اهتمامات مصمم نظام التشغيل ويجب على مبرمج التطبيق أيضًا تصميم آلية الحماية لحماية نظامهم من سوء الاستخدام.

السياسة تختلف عن الآلية Policy is different from mechanism تحدد الآليات كيف سيتم عمل شيء ما ، وتحدد السياسات ما سيتم القيام به. تتغير السياسات بمرور الوقت والمكان المناسب. الفصل بين الآلية والسياسة مهم لمرونة النظام.

الحماية في نظام الملفات Protection in File System

في أنظمة الكمبيوتر، يتم تخزين الكثير من معلومات المستخدم والهدف من نظام التشغيل هو الحفاظ على أمان بيانات المستخدم من الوصول غير الصحيح إلى النظام ويمكن توفير الحماية بعدة طرق

أنواع الوصول Types of Access

تحتاج الملفات التي لها وصول مباشر لأي مستخدم إلى الحماية ولا تتطلب الملفات التي لا يمكن الوصول إليها من قبل المستخدمين الآخرين أي نوع من الحماية. توفر آلية الحماية تسهيل الوصول المتحكم فيه فقط من خلال الحد من أنواع الوصول إلى الملف. يمكن منح حق الوصول أو عدم منحه لأي مستخدم بناءً على عدة عوامل أحدها هو نوع الوصول المطلوب. يمكن التحكم في عدة أنواع مختلفة من العمليات:

- **Read –** Reading from a file.
- **Write –** Writing or rewriting the file.
- **Execute –** Loading the file and after loading the execution process starts.
- **Append –** Writing the new information to the already existing file, editing must be end at the end of the existing file.
- **Delete –** Deleting the file which is of no use and using its space for another data.
- **List –** List the name and attributes of the file.

عمليات مثل إعادة التسمية وتحرير الملف الحالي والنسخ يمكن أيضًا التحكم فيها. هناك العديد من آليات الحماية. كل آلية منها لها مزايا وعيوب مختلفة ويجب أن تكون مناسبة للتطبيق المقصود.