الاسبوع الثاني عشــر

حماية المكونات المادية
Hardware Protection

حماية المكونات المادية Hardware Protection

نظام التشغيل يعمل بشكل جيد إذا كانت المكونات المادية جيدةً ، لذا يجب على نظام التشغيل حماية نفسه وحماية بقية البرامج من أن يطغى عليها برنامج آخر.

في النظام الدفعي batch operating إذا كانت حلقة loop غير منتهية وفيه قراءة ،ففي هذه الحالة سوف يقرأ بطاقة المهمة (Job1) ثم المهمة (Job2) ثم المهمة (Job3) ... وهكذا ، ويعتبرها معلومات أو بيانات لمهمة واحدة وبالتالي يحصل خطأ في عملية القراءة ، فيتطلب من نظام التشغيل أن يوقف مثل هذه الحالات غير الشرعية من خلال توفير حماية مدعومة بمكونات مادية .

كذلك يتطلب حماية برامج النظام وبرامج المستخدم من خلال مكونات مادية أيضا لحماية الذاكرة والمعالج والإدخال/الإخراج وحماية البرامج من بعضها البعض ، ويتم من خلال ما يسمى بعملية النمط المزدوج .

النمط المزدوج Dual Mode Operation

1- نمط المستخدم User Mode :

يكون التنفيذ لمصلحة المستخدم .

2- نمط النظام System Mode أو نمط المراقب (Monitor mode) ، أو نمط المشرف (Supervisor mode) أو النمط المميَّز (Privileged mode) : يكون التنفيذ لمصلحة نظام التشغيل.

عمل النمط المزدوج : تم إضافة Bit إلى مكونات الحاسوب يسمى (Mode Bit) لتحديد نمط العمل الحالي ، فإذا كانت قيمة الـ

Bit = 0 فأن التنفيذ لمصلحة النظام .

Bit = 1 فأن التنفيذ لمصلحة المستخدم .

- - - -	Mode Bit	- - - -

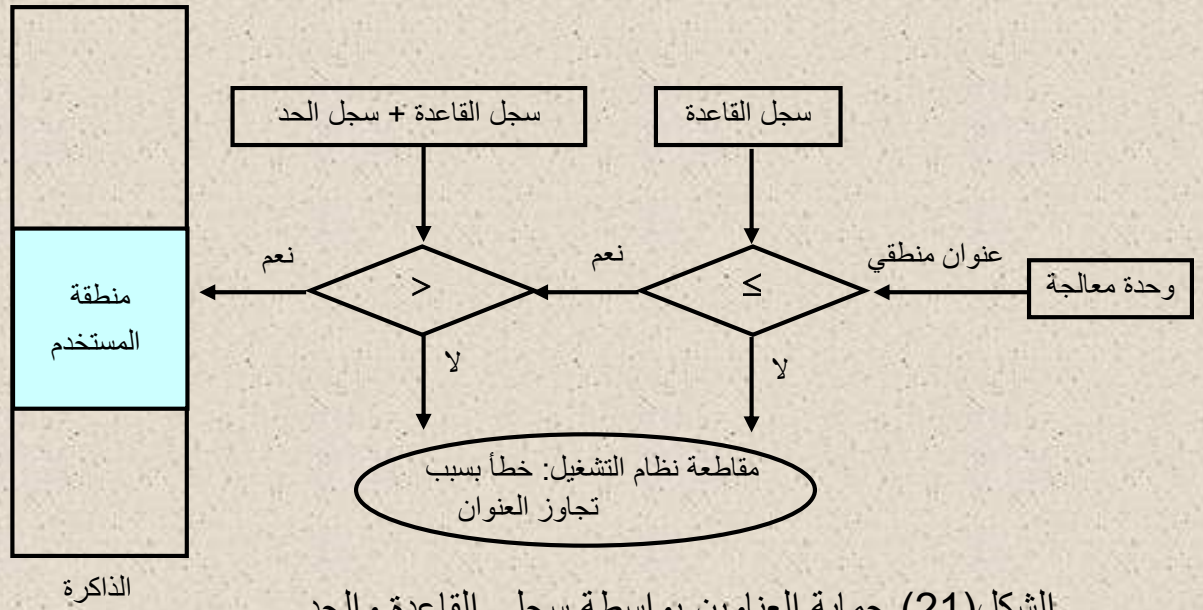
حماية الإدخال والإخراج I/O Protection

1- جميع إيعازات الإدخال والإخراج من الإيعازات ذات الامتياز التي تنفذ في نمط النظام لكي تمنع المستخدم من تنفيذ إدخال وإخراج غير شرعي . لذا يجب أن يكون نظام التشغيل هو المسيطر في كل عمليات الإدخال والإخراج ولا يمكن أبدا أن يكون المستخدم هو المسيطر لأنه من الممكن أن يكتب في أي موقع في الذاكرة فيحصل عندها خطأ . كما هي في حالة حصول مقاطعة بحيث أن الكتابة في موقع في الذاكرة قد تؤدي إلى حصول خطأ في عنوان خدمة المقاطعة وبذلك تكون الخدمة من عنوان خاطيء .

2- إحدى الايعازات ذات الامتياز هو الإيعاز المستخدم لتغيير قيمة (Mode Bit) وذلك لكي لا يستطيع المستخدم من الوصول له وتغيير قيمته ، لذا يكون نظام التشغيل هو المتحكم في التغيير أعلاه فقط .

حماية الذاكرة Memory Protection

لأجل ضمان عمل صحيح ، لابد من حماية جدول متجه المقاطعة (IVT) الذي يحوي أرقام المقاطعات من التعديل من قبل برنامج المستخدم ،بالإضافة إلى حماية روتين خدمة المقاطعة (ISR) من التعديل في نظام التشغيل ، ويمكن إجراء هذه الحماية من خلال استخدام سجلين وهما سجل القاعدة (Base Register) وسجل الحد (Limit Register) ، كما في الشكل (21) والشكل (22) أدناه :



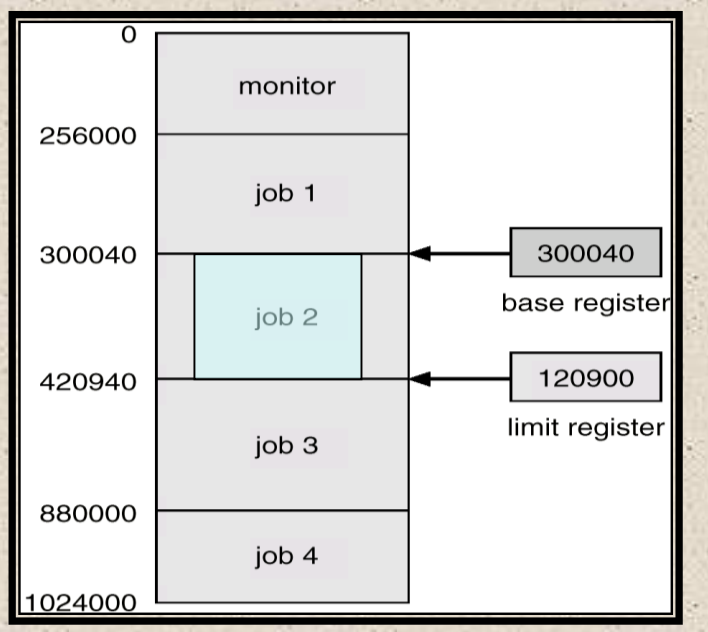
الشكل(21) حماية العناوين بواسطة سجلي القاعدة والحد

سجل القاعدة *Base Register* :

يحمل أقل عنوان فيزيائي مسموح الكتابة والخزن في عناوين الذاكرة .

سجل الحد *Limit Register* :

يحوي حجم البرنامج أو المهمة الموجودة في الذاكرة .



الشكل(22) يوضح قيمة سجلي القاعدة والحد

حماية وحدة المعالجة المركزية CPU Protection

نظام التشغيل يجب أن يكون هو المسيطر ، يجب أن يمنع برنامج المستخدم من الحصول على السيطرة والتنفيذ لوجود حلقة Loop غير منتهية وعدم إعادة السيطرة إلى نظام التشغيل ، لذا تم استخدام تقنية المؤقت (Timer) من خلال مقاطعة يتم تفعيلها .

ما هي الأغراض الرئيسية من استخدام تقنية المؤقت في حماية المعالج :

1- يمنع برنامج المستخدم من التنفيذ غير المنتهي . كيف ؟
هناك حالات يبقى برنامج المستخدم يعمل بدون وقت محدد (غير منتهي) وهذا الوقت الإضافي في التنفيذ يكون من وقت المعالج الثمين ، لذلك يوضع مؤقت من خلال عداد (Counter) يوضع فيه (n) من الوقت وتحدد قيمة (n) بأكبر وقت مسموح للبرنامج للتنفيذ ، وكلما يتم تنفيذ البرنامج يتم إنقاص قيمة العداد إلى أن تصل قيمة العداد إلى الصفر (0) عندها ستحدث مقاطعة لتوقف عمل البرنامج الحالي والتخلي عن المعالج .
2- إن المؤقت يولد مقاطعة بعد كل شريحة زمنية (Time Slice) بحيث أن كل مستخدم يسمح له بتنفيذ برنامجه ضمن الشريحة الزمنية المخصصة له وإلاّ تحصل مقاطعة ويتم تحويل السيطرة أو التنفيذ للبرنامج الثاني ومنحه المعالج .
3- حساب الوقت الحالي ،إذا كان لدينا مقاطعات عديدة وخلال كل ثانية تحصل مقاطعة (مقاطعة/ثانية) فيمكن حساب وقت الانتهاء من جميع المقاطعات بدءا من لحظة حصول المقاطعات . ويمكن حساب الوقت من خلال تطبيق المثال :

<u>مثال:</u>
لنفرض وجود 1427 مقاطعة عند الساعة الواحدة بعد الظهر ، احسب الوقت النهائي بعد انتهاء المقاطعات من التنفيذ على افتراض حصول (مقاطعة/ثانية) ؟

<u>الجواب :</u>
1427 ÷ 60 = 23 دقيقة والباقي 47 ثانية. (عملية القسمة تجرى بطريقة القسمة الطويلة)
نضيف الناتج أعلاه إلى وقت بداية المقاطعات وكما معطى في المثال أعلاه عند الساعة الواحدة بعد الظهر لذا يكون كالآتي :

01:00:00
+ 00:23:47

الناتج 01:23:47 بعد الظهر (الوقت الحالي)

الفرق بين مصطلحي الحماية والأمن حسب منطق الحاسبات الالكترونية

The differences between protection and security in computer terminology

طرائق حماية البيانات:

1- استخدام كلمات المرور Passwords وتغييرها من حين لآخر.

2- استخدام دلائل التأكيد Authentication .

3- إعطاء اولويات وصلاحيات دخول Authorization للبيانات والبرمجيات والملفات وهذه الاولويات والصلاحيات تحدد من قبل الإدارة أو المؤسسة.

4- استخدام شفرات Codes مختلفة ذات معايير عالمية ومحلية للتقييد بها مثل عملية التشفير التي من شانها تحويل البيانات إلى نصوص غير مفهومة للمتطفلين ويفهما الطرف الآخر عن طريق حل هذه الشفرةDecryption

5- عمل نسخ احتياطية للملفات Backup .

6- وضع وسائط التخزين الثانوية من أقراص وأشرطة مغناطيسية وغيرها في غرف خاصة.

7- استخدام البرامج الكاشفة للفيروسات وتحديث هذه البرامج لتواكب أنواع الفيروسات الجديدة التي قد تظهر.

بيئة الأمان:

يستخدم بعض الناس مصطلحات الأمان والحماية بشكل متداخل، ولتجنب الإرباك يستخدم مصطلح الأمان security للإشارة إلى المشكلة ككل ومصطلح الحماية protection للإشارة إلى آليات نظام التشغيل الخاصة المستخدمة لحماية المعلومات في الحاسوب.

للامان عدة وجوه، أهم ثلاثة وجوه هي طبيعة التهديدات وطبيعة الاختراقات (المتطفلون) والفقدان العرضي للمعلومات.

1- التهديدات:

من ناحية الأمان فان للحاسوب ثلاثة أهداف رئيسية وكما في الجدول(4) الأهداف والتهديدات الموافقة لها. يجب أن تبقى البيانات سرية لأشخاص محدودين دون غيرهم ،يجب أن لا يتمكن المستخدمون غير المرخص لهم من تعديل البيانات بدون إذن المالك من حذف أو إضافة بيانات خاطئة ايضاً. أما جاهزية النظام تعني أن لا يتمكن أي شخص من التشويش و الإخلال بالنظام.

2- المتطفلون:

معظم الناس صالحون ويتبعون القوانين. لذا لماذا القلق بشأن الأمان ؟ بسبب وجود بعض الأشخاص غير الجيدين والذين يَودّون التسبب بالمشاكل .

في علم الأمان، يدعى الأشخاص الذين يتواجدون في الأماكن التي لا عمل لهم فيها بالمتطفلين أو الأعداء. يعمل المتطفلون بطريقتين مختلفتين، يريد المتطفلون السلبيون قراءة الملفات غير المرخص لهم بقراءتها فقط، في حين أن المتطفلين الفعالين أكثر مكراً إذ يَودّون أجراء تغييرات غير شرعية على البيانات.

الجدول(4) يوضح الهدف والتهديد من ناحية أمان الحاسوب

الهـدف	التهديــد
سرية البيانات	فضح البيانات
تكامل البيانات	التلاعب بالبيانات
جاهزية النظام	رفض الخدمة

3- ضياع البيانات العرضي:

بالإضافة إلى التهديدات التي يتسبب بها المتطفلون الماكرون ، يمكن للبيانات القيّمة أن تفقد بطريق الخطأ أو الصدفة. وهناك أسباب للضياع العرضي للبيانات منها:

1- القضاء والقدر.

2- أخطاء البرامج أو الماديات الصلبة.

3- الأخطاء البشرية.

يمكن التعامل مع معظم هذه المسائل بالتخزين الاحتياطي المناسب ويفضل أن يكون بعيداً عن البيانات الأصلية.

اسئلة اختبارية :

س1: عمل النمط المزدوج في حماية المكونات المادية للحاسوب يتم من خلال وجود Bit يسمى 0000000 , اذا كانت قيمة الـ Bit تساوي 000000 فان التنفيذ لمصلحة 0000000 وإذا كانت القيمة تساوي 000000 فان التنفيذ لمصلحة 0000000؟

س2: سجل الحد .Limit reg في حماية الذاكرة يحوي 00000000000000000000000000

س3: عدد طرائق حماية البيانات ؟

س4: في بيئة الامان فان للحاسوب اهداف ؟ اذكر كل هدف مع طبيعة التهديدات الموافقة للهدف ؟