Chapitre 12

Niveaux de privilège

Nous avons utilisé le mode « protégé » sans, pour l'instant, en avoir justifié le nom. La dernière caractéristique de ce mode, que nous allons étudiée dans ce chapitre, va justifier cette dénomination.

12.1 Protections des systèmes d'exploitation multitâches

Nous avons vu depuis longtemps, en tant qu'utilisateur, l'intérêt d'un système d'exploitation multitâche et, dans une moindre mesure peut-être, celui d'un système multi-utilisateurs. Nous avons vu, dans le chapitre précédent, le principe de la mise en place d'un système multitâche. Nous n'avons, pour l'instant, pris aucune mesure de protection particulière pour un tel système.

Problèmes de conception des systèmes multitâches.- L'exécution en parallèle suppose une coexistence harmonieuse des tâches en cours, chacune d'elles devant se garder d'empiéter sur la mémoire gérée par l'autre. Une façon de faire est d'isoler les tâches les unes des autres, le système d'exploitation devant lui aussi être protégé contre l'incursion des programmes et de leurs différentes tâches.

Problèmes de conception des systèmes multi-utilisateurs.- Dans un système multi-utilisateurs, on veut que, à côté de fichiers partagés, chaque utilisateur puisse possèder des fichiers en propre, non accessibles par les autres utilisateurs. Il faut donc prévoir un procédé de *protection des fichiers* et, plus généralement, de *protection des ressources* : il ne faut pas, par exemple, que l'utilisateur A détruise des données de l'utilisateur B en mémoire centrale, que ce soit par inadvertance ou de façon délibérée.

Aides logicielle et matérielle.- On peut concevoir un tel système d'exploitation de façon purement logicielle, par exemple à l'aide du mode réel des microprocesseurs *Intel*. Cependant, les utilisateurs astucieux peuvent toujours trouver comment passer outre. La protection des données de façon matérielle, et non plus logicielle, est plus sûre.

Notion de niveau de privilège.- Une façon matérielle de faire est de mettre à la disposition du programmeur plusieurs **niveaux d'utilisateurs** ou **niveaux de privilège**, ceux-ci permettant de restreindre l'accès à la mémoire et aux ports d'entrées-sorties : un utilisateur de niveau inférieur (le niveau zéro est considéré comme celui qui a tous les droits) peut accéder aux données d'un utilisateur de niveau supérieur, mais l'inverse est interdit, sauf s'il est explicitement permis.

Cas des microprocesseurs *Intel*.- Il existe quatre niveaux de privilège, numérotés de 0 à 3, depuis le 80286.

Cependant les systèmes d'exploitation, que ce soit *Windows* ou *Linux*, n'utilisent que les niveaux 0 et 3. Pour reprendre le vocabulaire de *Linux*, le niveau 0 est utilisé dans le **mode noyau** du système d'exploitation, dit aussi **niveau système**, le niveau 3 est le **mode utilisateur**.

Types de programmation.- On distingue, lorsqu'il existe plusieurs niveaux de privilège, deux types de programmation : la *programmation des applications* et la *programmation système*.

— Dans le cas de la **programmation des applications**, on n'a pas accès librement à la mémoire (pas d'accès aux registres de segment et à certains autres registres pour *Intel*), on a un accès limité aux entrées-sorties (la plupart du temps il faut faire appel aux seules routines permises par le niveau système) et les *adresses* mémoire sont *virtuelles* : elles ne correspondent pas aux *adresses physiques* et l'utilisateur n'a aucun moyen de connaître les adresses physiques auxquelles elles correspondent, le système d'exploitation en faisant le lien.

— Dans le cas de la **programmation système**, au niveau de privilège 0, on a tous les droits. Mais une fois le programme lancé, le système d'exploitation en général, on ne peut plus programmer à un tel niveau en général, y compris le super-utilisateur.

Dans le cas des microprocesseurs *Intel*, la programmation système se fait soit en mode protégé niveau zéro, soit en mode réel. Ce dernier point explique pourquoi on ne peut pas accéder au mode réel en programmation des application sur un système d'exploitation ayant choisi d'utiliser les niveaux de privilège, et en particulier que l'on ne peut plus avoir accès aux interruptions du BIOS ou du DOS.

12.2 Instructions en mode protégé

Nous avons déjà vu quelques instructions relatives au mode protégé : celles permettant le passage du mode réel au mode protégé ou *vice-versa*. Elles ne peuvent être exécutées qu'en mode réel ou en mode protégé avec le niveau de privilège 0 :

Instruction	**Fonction**
SGDT	Rangement de la table globale des descripteurs
SIDT	Rangement de la table des descripteurs d'interruption
LGDT	Chargement de la table locale des descripteurs
LIDT	Chargement de la table des descripteurs d'interruption
LMSW	Chargement du MSW
SMSW	Rangement du MSW

Les instructions relatives à la mise en œuvre du multitâche et aux protections ne s'exécutent qu'en mode protégé (pas en mode réel) avec le niveau de privilège 0. Une exception 6 est levée lorsqu'on tente de les exécuter en mode réel ou virtuel :

Instruction	**Fonction**
STR	Rangement du registre de tâche
SLDT	Rangement de la table locale des descripteurs
LTR	Chargement du registre de tâche
LLDT	Chargement de la table locale des descripteurs
ARPL	Ajustement du niveau de privilège requis
LAR	Chargement de l'octets des droits d'accès
LSL	Chargement de la limite du segment
VERR	Vérification du segment pour lecture
VERW	Vérification du segment pour écriture