

Extrait du Spyworld Actu

<http://spyworld.spyworld-actu.com/spip.php?article733>

# Dérive sécuritaire pour le bus PCI Express 2.0

- Informatique - Hardware -



Date de mise en ligne : vendredi 9 septembre 2005

---

Spyworld Actu

---

### **Cette nouvelle version améliorera la vitesse et simplifiera la virtualisation. Mais elle introduit un mouchard plutôt gênant.**

Il y a des avancées technologiques dont on préférerait se passer. Notamment celles qui présentent un danger pour le libre arbitre, qui brident nos choix. C'est exactement ce qui pourrait se produire avec PCI Express 2.0, la future évolution du bus PCI Express (PCIe). Ses premières spécifications viennent d'être présentées par Intel.

Comme toujours, la vitesse augmente, les débits aussi et de nouvelles fonctions plus ou moins intéressantes font leur apparition. Mais l'une d'elles retient un peu plus l'attention : l'introduction d'un mécanisme de certification des périphériques et des flux d'entrée/sortie.

Qu'est-ce que cela signifie ? Que les logiciels pourront « identifier de façon unique un périphérique » et s'assurer que celui-ci est certifié. A l'inverse, le périphérique pourra « distinguer si les requêtes viennent d'un logiciel qui est certifié ou non » et agir en conséquence. Et c'est l'utilisateur qui pourrait en faire les frais. Sans agiter les épouvantails, il est facile d'imaginer qu'un fabricant de machines bloque l'installation de périphériques venant d'un autre constructeur. Pire, certains adaptateurs réseaux ou cartes SCSI pourraient ne plus fonctionner qu'avec telle ou telle application.

Bien entendu, Intel s'en défend. « Le système d'exploitation est en proie à de plus en plus d'attaques directes des entrées/sorties. PCIe 2.0 offrira une protection matérielle beaucoup plus efficace que n'importe quel logiciel », justifie David Harriman, architecte du fondeur. Certes, mais comment garantir qu'il n'y aura pas de dérives ?

#### **Maintenir l'utilisateur sous sa coupe**

Les fournisseurs invoquent souvent la sécurité, la protection contre les virus et le piratage pour justifier ce genre de mécanismes. Mais l'expérience prouve qu'ils s'en servent plutôt pour garder un contrôle total en décidant qui est certifié et qui ne l'est pas. Au final, il s'agit plus de maintenir l'utilisateur sous sa coupe que de garantir sa sécurité.

#### **Une virtualisation simple et efficace**

Ce virage sécuritaire est d'autant plus regrettable que PCIe 2.0 introduit plusieurs évolutions vraiment intéressantes. La virtualisation autorisera, par exemple, à plusieurs systèmes d'exploitation de partager facilement les périphériques d'une machine. On virtualise, en effet, très bien les processeurs et la mémoire.

Mais dès qu'il s'agit des entrées/sorties, il faut installer des pilotes complexes adaptés à du matériel spécifique. La prise en charge de la virtualisation par le bus PCI simplifiera grandement la tâche. Elle améliorera aussi les performances puisque tout est géré directement par le matériel.

Rappelons que la ratification finale de PCIe 2.0 est attendue pour le deuxième trimestre 2006, pour un début des tests fin 2006. Certaines fonctions peuvent encore être revues, édulcorées voire abandonnées comme l'ont été le numéro de série du Pentium ou l'initiative Palladium de Microsoft.

## Des cartes mini PCI tatouées

Plusieurs fabricants de portables brident le Bios de leurs machines pour qu'elles n'acceptent que les périphériques de leur catalogue. C'est le cas des cartes mini PCI des portables HP ou des lecteurs de CD USB du X30 d'IBM. De même, des cartes audio bloquent l'enregistrement, dès qu'elles rencontrent un flux protégé.

## Quoi de neuf dans PCIe 2.0 ?

Totalement compatible avec PCIe 1.x. Fréquence qui passe de 2,5 à 5 GHz. Bande passante doublée à 5,0 GT/s. Consommation réduite. Certification des périphériques. Virtualisation des périphériques. Gestion de la qualité de service. Nouveaux connecteurs : cartes ultrafines pour portables et fonds de panier pour les serveurs lames ou briques.