Un anti-rootkit signé Intel

Intel développe un composant qui sera implémenté sur le 'chipset' et qui permettra de surveiller le système d'exploitation et les applications afin de détecter les tentatives de modification de la mémoire ou du code.

Les '*rootkits*' sont ces programmes insidieux et rarement détectés par les antivirus, qui se cachent dans les OS ou les applications à l'insu de l'utilisateur et qui peuvent enregistrer les actions de ce dernier, modifier les applications et même créer des trous dans la protection des systèmes. Pour Intel, tout ce qui ne s'apparente pas à ce mode opératoire relève des antivirus, que sa technologie devrait donc compléter. Il en est ainsi de sa technologie '*LaGrande*', ici aussi un 'chip' (composant) de sécurité TPM (*Trusted Platform Mobile*) qui rejoindra prochainement le chipset. '*LaGrande*' permettra d'isoler les blocs de mémoire les un des autres, afin de prévenir tout risque de pollution de l'un vers l'autre. Elle permettra aussi de crypter les informations directement sur les '*buffers*' (mémoires temporaires) graphiques ou du clavier. Cependant, cette technologie a ses limites, car elle protège les données et le code des menaces qui proviennent de l'extérieur, mais pas des menaces internes cachées, comme les 'rootkits'. C'est pourquoi la nouvelle technologie d'Intel, annoncée pour 2008/2009, devrait probablement rejoindre 'LaGrande 2', la prochaine version de la protection du fondeur, et la compléter en apportant les deux niveaux de protection hardware.