Proposition de recherche doctorale

Création-destruction dynamique de machines virtuelles sécurisées sur une architecture manycore cc-NUMA

Mots clés :

- **Directeur de thèse** : Alain Greiner
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Depuis le milieu des années 2000, la performance des processeurs n'est plus liée à l'accroissement de la vitesse des processeurs mais à l'accroissement du nombre de coeurs de processeurs intégrés. L'ITRS prévoit ainsi 1000 coeurs intégrés en 2020. Les systèmes informatiques, tels que les PCs, tablettes, téléphones, et bientôt les objets (maisons, voitures), sont de plus en plus connectés et ils hébergent des applications dont la provenance n'est pas toujours connue ou alors, exécutent des requêtes de clients parfois malveillants. La quantité de données qui circulent sur les réseaux est en progression rapide et transportent des informations sensibles qui doivent être protégées. Les futures plateformes manycore contenant plusieurs milliers de coeurs doivent offrir des garanties de sécurité alors même que l'exécution en parallélisme réel accentue le risque de créer des canaux cachés entre applications ou entre machines virtuelles s'exécutant sur la même plate-forme matérielle. L'enjeu est de proposer des garanties de sécurité renforcée aux applications sensibles s'exécutant sur ce type d'architecture. Ces questions ont été abordées avec des techniques différentes dans la thèse de Joël Porquet, pour des architectures multicore hétérogènes, ou dans la thèse de Geoffrey Plouviez, pour des architectures manycore homogènes. Cependant, dans un cas comme dans l'autre, la création des machines virtuelles cohabitantes et l'allocation des ressources à ces machines virtuelles étaient réalisées de façon statique au démarrage de la machine par un hyperviseur possédant le contrôle total de la plateforme. On souhaite dans cette nouvelle thèse introduire un fonctionnement plus dynamique en étudiant les mécanismes permettant de démarrer une nouvelle machine virtuelle ou arrêter une machine virtuelle en cours d'exécution sans ré-initialisation globale de l'ensemble de la plateforme. Les services que nous souhaitons garantir sont la confidentialité et l’intégrité des données manipulées par ces applications et la disponibilité des ressources qui leur sont attribuées (processeurs, segments de mémoire et périphériques), voire la qualité de service sur les canaux de communications entre applications. Nous souhaitons rendre l’architecture sécurisée transparente pour le programmeur d’application, en partant de l’hypothèse que le programmeur d’application n’a pas conscience des spécificités de la plateforme sur laquelle son programme va s’exécuter.

Résumé du projet de recherche (Langue 2)

Cette thèse s’inscrit dans le projet TSAR où le LIP6 propose une architecture manycore cc-NUMA scalable jusqu’à 4096 coeurs, mais ces techniques de sécurisation manycore constitue un enjeu très actuel en particulier dans le cadre du cloud-computing.