Stages L3, M1 et M2 autour du proto-noyau Pip

Equipe 2XS, laboratoire CRIStAL, université de Lille 1

25 novembre 2016

Mots-clés : vérification formelle, système d'exploitation, Coq, noyau

Le proto-noyau Pip

Pip est un proto-noyau : il permet d'exécuter en mode utilisateur des noyaux, allant des hyperviseurs aux noyaux monolithiques. Pip est seul à s'exécuter en mode noyau et ne fournit que des appels système pour la gestion de partitions isolées de la mémoire et la gestion de base du flux de contrôle, réduisant ainsi la base de confiance à son strict minimum.

La logique de Pip est codée avec Gallina – le langage de l'assistant de preuve Coq – et la preuve formelle qu'elle assure l'isolation des partitions de la mémoire est en cours de développement. Pour des raisons d'efficacité, ce code est automatiquement traduit en code C autonome (*freestanding*), c'est-à-dire du code C qui peut s'exécuter directement sur le matériel sans faire appel à des librairies.

La partie dépendante de l'architecture de Pip est implémentée en C et en assembleur. Elle consiste en une mince couche donnant accès au matériel.

Stages

Des sujets de stages autour de Pip peuvent être élaborés sur mesure en fonction des intérêts et du niveau des candidats. Il peuvent être centrés sur des aspects soit système soit formels et porter soit sur Pip soit sur son écosystème. Par exemple :

— certification de la traduction de Gallina vers C,
— vérification formelle de la partie dépendante de l'architecture,
— spécification formelle de l'API de Pip,
— impact de Pip sur les propriétés temps-réel,
— portage multicœur.

Pour aller plus loin

Télécharger Pip : `http://pip.univ-lille1.fr`

Contact : David Nowak (`david.nowak@univ-lille1.fr`)