Sujet de stage de Master :
Réalisation d'outils pour le décodage d'exécutables

(Informatique, stage de 4 à 6 mois)

- Thématiques : Informatique, langages machine, assembleur
- Mots clés : langage intermédiaire, outils de décodage, PowerPC, ARM
- Institut d'accueil : CEA LIST (Saclay, région parisienne, France)
- Encadrant : Sébastien Bardin (CEA)
- Contact encadrant : `sebastien.bardin@cea.fr`
- Lien Web : `http://sebastien.bardin.free.fr/stages.html`
- Durée : 4-6 mois. Rémunération : oui

La vérification automatique de programmes est reconnue comme l'un des grands challenges de la recherche en informatique. La plupart des techniques de vérification travaillent à partir du code source du programme, cependant il existe un besoin fort pour des outils de vérification travaillant directement à partir du code exécutable. Le projet ANR BINSEC [4] vise à construire de tels outils [1, 3], et notamment une plate-forme open-source pour le décodage d'un exécutable vers le langage intermédiaire formel des DBA [2], plus simple à analyser.

Sujet proposé. Le stagiaire participera au développement de la plate-forme BINSEC. Il travaillera plus particulièrement à la mise en place d'outils facilitant le décodage des exécutables vers les DBA. Les travaux attendus incluent :

- la participation à la mise au point d'un langage DSL dédié à la création de décodeurs, et des outils d'analyse associés (ex : typage) ;
- l'utilisation du DSL pour implanter un décodeur pour au moins une architecture parmi x86, ARM et PowerPC ;
- la mise en place d'un framework de test pour s'assurer que le décodage est correct, par exemple en s'interfaçant avec QEMU.

Le langage de travail sera principalement OCaml.

Références

[1] Bardin, S., Herrmann, P. : OSMOSE : Automatic Structural Testing of Executables. International Journal of Software Testing, Verification and Reliability (STVR), 21(1), 2011

[2] Bardin, S., Herrmann, P., Leroux, J., Ly, O., Tabary, R., Vincent, A. : The BINCOA Framework for Binary Code Analysis. In : CAV 2011. Springer, Heidelberg (2011)

[3] Bardin, S., Herrmann, P., Védrine, F. : Refinement-based CFG Reconstruction from Unstructured Programs. In : VMCAI 2011. Springer (2011)

[4] `http://binsec.gforge.inria.fr/`