Preuve d'un vérifieur de byte code JavaCard : métriques et retour d'expérience.

L. Burdy
GEMPLUS
Avenue du Pic de Bertagne - 13881 Gémenos Cedex - France
lilian.burdy@gemplus.com

14 juin 2002

La politique de sécurité des Java Card s'appuie sur différents composants tels que la machine virtuelle, l'API, le vérifieur, le chargeur de fichier, etc. Il est de toute évidence important que ces composants soient implémentés de manière à être en concordance avec leurs spécifications. Dans ce cadre, le projet européen Matisse a pour but objectif de proposer une méthodologie et des outils pour le développement d'applications industrielles à l'aide de la méthode B. L'un des cas d'étude du projet concerne la modélisation et la preuve de l'implémentation d'un vérifieur de byte code Java Card.

Le vérifieur a pour objectif, dans le schéma Java Card, de s'assurer que les applets chargées dans la carte pourront être exécutées de manière sûre. Pour cela il vérifie qu'elles sont structurellement cohérentes et que le byte code qu'elles contiennent est correctement typé. Cela consiste, par exemple, à s'assurer qu'il n'y aura pas de débordement de la pile, que les résultats des sauts restent confinés dans la méthode courante, etc. Le vérifieur est découpé en deux parties, une première s'assure des contraintes structurelles tandis que la seconde réalise la vérification du typage.

Nous nous intéresserons, ici, uniquement à cette deuxième partie, appelée vérifieur de type qui a été intégralement modélisée à l'aide de la méthode B et prouvée dans sa quasi-totalité.

En ce qui concerne les métriques, ce développement est représentatif d'un développement industriel. Il a en effet nécessité l'écriture de 20000 lignes de B réparties dans 34 composants différents. La preuve de ces composants génère 18160 obligations de preuve prouvées à 70 % par la preuve automatique de l'Atelier B. Ce développement a donc demandé de prouver interactivement plus de 5000 lemmes.

Cet exposé a deux objectifs. D'une part nous fournissons des métriques concernant cette campagne de preuve interactive avec un suivi au jour le jour de la progression de la preuve (nombres de lemmes générés, nombre de lemmes prouvés) mettant en évidence les différentes étapes de cette phase du développement. D'autre part, nous tenterons de définir, à partir de cette étude, un début de méthodologie permettant de mener à bien la preuve de tels projets.

Références :

Formal Development of an Embedded Verifier for Java Card Byte Code, Ludovic Casset, Lilian Burdy, Antoine Requet. DSN 2002. Washington (USA), Juin 2002.

Development of an Embedded Verifier for Java Card Byte Code using Formal Methods, Ludovic Casset. FME 2002. Copenhague (Danemark), Juillet 2002.