Rapport d'Activité de collaboration régionale Cône Sud-France: Cartes à Puce

1 Contexte et Objectifs

Le projet de collaboration a pour but de faciliter la spécification et vérification de la plateforme JavaCard, ainsi que le développement d'applications JavaCard certifiées. Les objectifs annoncés du projet étaient :

- **la spécification formelle des composantes de la plate-forme JavaCard.** C'est un préalable à toute vérification sur la plate-forme ou les applications.
- **le développement, l'instrumentation et l'intégration de méthodes de vérification de programmes.** Nous avions proposé de nous appuyer sur la spécification formelle de la plate-forme JavaCard pour vérifier des propriétés sur les applications JavaCard.
- **l'application des méthodes et outils développés à des cas d'étude issus du monde industriel.** d Nous avions proposé e confronter les résultats scientifiques du projet à des problèmes concrets issus du monde industriel.

2 Visites et participation à des conférences

2.1 Visites

- Juillet-Aout 2001 : Gilles Barthe a visité l'INCO et le FAMAF dans le but d'initier la collaboration autour des cartes à puce.
- Septembre 2001-Mars 2002 : Daniel Perovich a visité l'INRIA Sophia-Antipolis pour travailler sur la détection statique d'exceptions de sécurité pour JavaCard. Ces travaux se sont effectués sous la supervision conjointe de Gilles Barthe et Gustavo Betarte.
- Novembre 2001 : Marieke Huisman a visité l'INCO et le FAMAF dans le but d'initier la collaboration autour des cartes à puce.
- Février-Mai 2002 : Leonardo Rodríguez a visité l'INRIA Sophia-Antipolis pour travailler sur un algorithme d'élimination des sous-routines dans JavaCard.
- Mars 2002 : Daniel Fridlender a visité l'INRIA Sophia-Antipolis pour travailler sur la vérification par le typage des propriétés de sécurité des applications JavaCard.

- 17 Novembre 2002-13 Février 2003 : Tamara Rezk visite l'INRIA Sophia-Antipolis dans le but de définir un vérificateur de bytecode renforcé qui garantit la confidentialité des applications JavaCard.
- 1-13 Février 2003 : Pedro D'Argenio visitera l'INRIA Sophia-Antipolis dans le but d'étudier l'intégration d'outils de model-checking et d'assistants de preuves.
- Février 2003 : Leonor Prensa visitera l'Université de Rio Cuarto dans le cadre de l'école d'été en Informatique de Rio Cuarto.

2.2 Cours

- Juillet 2001, Montévideo : Gilles Barthe a donné un cours sur les assistants à la preuve et sur leurs applications à la sémantique des langages de programmation. Le but du cours était de familiariser les étudaints avec les outils et techniques de preuve utilisées par le consortium européen VerifiCard pour valider la plateforme JavaCard.
- Octobre 2001, Sophia-Antipolis : Daniel Perovich a donné un cours de 3e cycle sur la programmation d'applications JavaCard, et sur le modèle de sécurité de JavaCard 2.1. L'objectif du cours était de familiariser les doctorants du projet Lemme aux techniques de programmation pour les applications cartes à puce.
- Novembre 2001, Montévideo : Marieke Huisman a donné un cours de 3e cycle sur la vérification de programmes Java en logique d'ordre supérieur. L'objectif du cours était de familiariser les participants à une méthodologie de vérification formelle pour les applications JavaCard, et d'illustrer son application à des cas d'étude issus du monde industriel.
- Février 2003, Rio Cuarto : Leonor Prensa donnera un cours à l'école d'été en Informatique de Rio Cuarto sur la vérification de programmes parallèles. L'objectif du cours est de familiariser les étudiants aux techniques de vérification compiositionnelle basées sur les méthodes de Owicki-Gries et de "Assume-Guarantee".
- Juillet 2003, Montévideo : Gilles Barthe et Eduardo Giménez donneront un cours à l'ecole d'hiver UNESCO CIMPA sur la Sémantique Appliquée. L'objectif du cours est de familiariser les étudiants aux applications industrielles des méthodes formalles dans le domaine des cartes à puce et des petits objets sécurisés.

2.3 Exposés

- Aout 2001, Cordoba : Gilles Barthe a présenté les travaux de l'INRIA au sein du consortium européen VerifiCard.
- Novembre 2001, Cordoba : Marieke Husiman a présenté ses travaux sur la vérification compositionnelle de propriétés de sécurité pour les cartes à puce multi-applications.
- Octobre 2001, Daniel Perovich a présenté ses travaux sur une méthodologie de développement d'applications sécurisées pour JavaCard.

- Mars 2002, Daniel Perovich a présenté ses travaux sur la détection statique d'exceptions de sécurité dans JavaCard.
- Janvier 2003, Sophia-Antipolis : Tamara Rezk présentera ses travaux de DEA sur la logique de Reynolds pour la vérification de programmes impératifs.
- Février 2003, Sophia-Antipolis : Pedro D'Argenio présentera ses travaux de recherche sur la vérification de systèmes temps réel.

2.4 Participations à des conférences

- Septembre 2001, Cannes : Daniel Perovich a participé en tant qu'auditeur à 'e-Smart 2001'.
- Janvier 2002, Marseille : Daniel Perovich a participé en tant que conférencier à 'VerifiCard 2002', où il a présenté un travail intitulé 'A Simple Methodology for Secure Object Sharing in Java Card', par Perovich, Rodriguez, Varela.
- Avril 2002, Grenoble : Leonardo Rodríguez a participé en tant qu'auditeur à 'ETAPS 2002'.

2.5 Divers

Gilles Barthe est membre du comité de programme de WAIT 2003 : Workshop Argentino de Informatica Teorica, et organisateur de l'école d'hiver UNESCO CIMPA sur la Sémantique Appliquée.

Gustavo Betarte est membre du comité scientifique et co-organisateur de l'école d'hiver UNESCO CIMPA sur la Sémantique Appliquée.

Alberto Pardo est co-organisateur de l'école d'hiver UNESCO CIMPA sur la Sémantique Appliquée.

3 Travaux scientifiques réalisés

3.1 Détection statique d'exceptions de sécurité

Daniel Perovich a raffiné la méthodologie de développement d'applets sécurisés pour la rendre applicable à un cas d'étude proposé par Gemplus. Ces travaux ont donné lieu à une publication dans les actes informels de "VerifiCard 2002".

Daniel Perovich a également développé une analyse statique des programmes Java(Card) qui détecte toute violation du mécanisme de pare-feu qui pourrait conduire à la levée d'exceptions de sécurité. Ce travail a débouché sur l'implémentation d'un prototype, et constituera le corps de son mémoire de Mestrado.

3.2 Non-interférence par vérification de bytecode

Daniel Fridlender a conduit une étude préliminaire sur l'utilisation des systèmes de type pour la vérification des propriétés de sécurité des applications

Java et JavaCard : confidentialité et disponibilité. A l'issue de cette étude, Gilles Barthe et Daniel Fridlender ont conjointement décidé de s'attaquer au problème de la non-interférence pour JavaCard (la non-interférence garantit la confidentialité des applications). Gilles Barthe, Leonor Prensa, et Tamara Rezk poursuivent actuellement cet axe de recherche, et ont défini un système de types pour contrôler le flux d'information dans la machine virtuelle Java(Card). Le travail porte actuellement sur une preuve de la non-interférence, et sur sa formalisation dans un assistant à la preuve. Deux articles de conférence sont actuellement en préparation.

3.3 Elimination des sous-routines dans JavaCard

Leonardo Rodríguez a étudié le problème des sous-routines, pour lesequelles la vérification de bytecode est notoirement complexe. Il a en particulier analysé différents algorithmes d'élimination des sous-routines, et a démontré d'une part que certains algorithmes proposés dans la litérature ne sont pas corrects dans la mesure où ils ne préservent pas la sémantique des programmes, et d'autre part qu'il existe un algorithme correct. La preuve de correction de ce dernier algorithme a été établie dans le cadre de l'assistant à la preuve Coq, en s'appuyant sur les modèles formels de la machine virtuelle JavaCard développé par l'équipe Lemme.

Ce travail a débouché sur la rédaction d'un rapport technique qui servira de base à la rédaction de son mémoire de Mestrado.