Propuesta de proyecto de cooperación regional (Cono Sur) y Francia: Tarjetas Inteligentes

Gilles Barthe, Gustavo Betarte, Daniel Fridlender, Alberto Pardo

1 Descripción del proyecto y objetivos perseguidos

Proponemos un proyecto de cooperación que permita facilitar la especificación y verificación de políticas de seguridad de programas JavaCard, así como la implementación de prototipos de diferentes componentes de esta tecnología y el desarrollo de aplicaciones.

Contexto

Numerosos campos de aplicación de la Internet y de las tarjetas inteligentes, en particular y en forma paradigmática el comercio electrónico, requieren que datos y recursos sean protegidos por medio de mecanismos de seguridad sofisticados.

El lenguaje de programación Java representa una respuesta práctica a las cuestiones de movilidad y seguridad sobre Internet, y a través de JavaCard, para la programación de tarjetas inteligentes. Actualmente, se puede afirmar que Java se ha impuesto como un estándar de facto en estos dominios de aplicación donde las exigencias de seguridad son muy altas.

La seguridad de programas Java debe ser abordada a diferentes niveles. Ante todo, es necesario establecer propiedades de seguridad del lenguaje, notablemente la propiedad de *type safety* que garantiza que ciertos programas que podrían presentar comportamientos erróneos en tiempo de ejecución no sean aceptados por el compilador. También es importante establecer propiedades sobre el gestionamiento de la memoria a ser utilizada por un ambiente de ejecución de aplicaciones Java y de qué forma son compartidos los datos por diferentes aplicaciones al ser éstas ejecutadas en dicho ambiente.

La actividad de investigación a ser desarrollada en este proyecto pretende focalizarse fundamentalmente en el entendimiento, formalización y desarrollo de herramientas que sean utilizadas para la generación de aplicaciones confiables en el marco de la tecnología de tarjetas inteligentes, y particularmente en el contexto JavaCard.

Objetivos

En el marco de un ambiente para la verificación de políticas de seguridad de aplicaciones JavaCard, así como para el diseño e implementación de esas aplicaciones, se identifican los siguientes objetivos generales:

- la especificación formal de los componentes involucrados en la ejecución de aplicaciones del tipo que nos concierne;
- la identificación, formulación y verificación de propiedades de seguridad a ser requeridas sobre esos componentes;
- el diseño e implementación de ambientes integrando varios métodos de verificación, tal como *proof editors* y *model-checkers*.

Más precisamente, los objetivos específicos del proyecto son los siguientes:

- **Modelización y Especificación Formal de la Plataforma JavaCard (JCVM):** éste es un prerrequisito indispensable para poder hacer efectiva la verificación de políticas de seguridad. Se considera deseable modelar la Maquina Virtual JavaCard, el Runtime Environment (JCRE) y las correspondientes interfaces (APIs). A más largo plazo se podrá estudiar las funcionalidades que podrán ser integradas brevemente a JavaCard (multithreading, garbage collection), tal como una extensión de la formalización hacia la máquina virtual Java (JVM).
- **Especificación de Políticas de Seguridad:** en una primera etapa nos proponemos formular y probar propiedades concernientes a la gestión de la memoria y los mecanismos de *firewall* y object sharing.
- **Ambiente de verificación:** en el ambiente de Jakarta (desarrollado por el INRIA Sophia-Antipolis) se podrá considerar la instrumentación de métodos de abstracción y su integración con sistemas de ayuda para la certificación mecanizada de pruebas (*proof-editors*) así como con verificadores de modelos (*model-checkers*).

2 Acerca de los equipos de investigación

Los equipos de investigación que integran este proyecto son:

- el equipo francés está formado por investigadores del proyecto Lemme del INRIA Sophia-Antipolis (Gilles Barthe, Marieke Huisman), y tiene competencia en las áreas de sistemas de prueba, verificadores de modelos, análisis de programa, programación orientada a objetos y seguridad. Este equipo está desarrollando un ambiente de verificación de propiedades de seguridad de programas JavaCard, y está participando en varios proyectos académicos e industriales.

- el equipo uruguayo está formado por investigadores del Grupo de Métodos Formales del Instituto de Computación (InCo) de la Universidad de la República (Gustavo Betarte, Alberto Pardo). Este grupo ha concretado un cierto número de proyectos y publicaciones a nivel regional e internacional en torno a las tarjetas inteligentes. A su vez ha comenzado a consolidar relaciones a nivel académico con laboratorios de la región y de Francia así como empresas nacionales y multinacionales instaladas en Uruguay. En particular, este equipo esta desarrollando una aplicación, entre varios proyectos acordados, para el Hospital Universitario (Hospital de Clínicas) de la Universidad de la República que consiste en la informatización de registros clínicos basada en tarjetas inteligentes.

- el equipo argentino está formado por investigadores del Grupo de Métodos Formales de la Facultad de Matemática, Astronomía y Física de la Universidad de Córdoba (Daniel Fridlender, Javier Blanco, Pedro D'Argenio). Este grupo tiene experiencia en el uso de métodos formales en aplicaciones industriales, y si bien es de creación más reciente, ha concretado un cierto número de publicaciones internacionales en los temas de concurrencia, model-checking, sistemas de tiempo real.

  Se han iniciado contactos y se espera integrar al proyecto un laboratorio chileno y uno brasilero.

3 Antecedentes de colaboración con la contraparte francesa

Los investigadores Gilles Barthe, Gustavo Betarte y Daniel Fridlender formaron parte, en los años 97 y 98, del grupo de investigación de Lógica de la Programación (*ProgLog*) del Departamento de Ciencias de la Computación de la Universidad Tecnológica Chalmers de Gotemburgo, Suecia. Subsecuentemente se mantuvieron en contacto, por ejemplo con visitas (Barthe a Montevideo y Córdoba en el 2001, Betarte a INRIA Sophia-Antipolis en el 2000, y Fridlender a Montevideo e INRIA Rocquencourt en 2001).

4 Actividades programadas

Misiones de Francia a Cono Sur:
Marieke Huisman (INRIA Sophia-Antipolis) 15 días Noviembre 2001

El objetivo de la visita será el dictado de un curso de posgrado sobre la verificación de programas Java en lógica de orden superior. Este curso se dictará en Montevideo. Investigadores del equipo argentino se desplazarán a esa ciudad con el doble propósito de asistir al curso y participar en un workshop que será llevado a cabo durante la estadía de Marieke Huisman. La misión incluirá una visita de Marieke Huisman a Córdoba.

Misiones de Cono Sur a Francia:

Alberto Pardo (InCo, Montevideo)	1 semana	Septiembre 2001
Daniel Perovich (InCo, Montevideo)	6 meses	desde 15 de Sept. 2001
Daniel Fridlender (FaMAF, Córdoba)	1 mes	Enero 2002
Pedro D'Argenio (FaMAF, Córdoba)	1 mes	Febrero 2002
Carlos Luna (InCo, Montevideo)	1 mes	Febrero 2002

Alberto Pardo visitará Sophia-Antipolis para efectuar una selección y definición detallada de las actividades a desarrollarse en coordinación durante los primeros meses.

Daniel Perovich visitará Sophia-Antipolis para realizar una pasantía (étage) bajo la supervisión de Gilles Barthe y Gustavo Betarte. Esta pasantía tiene como principal objetivo dar lugar a la concepción y elaboración del trabajo de tesis de maestría de Daniel Perovich.

Daniel Fridlender efectuará una visita de trabajo con el propósito de evaluar en profundidad los resultados alcanzados hasta el momento y realizar un estudio comparativo de las técnicas y herramientas utilizadas y de la posibilidad de integrarlas. Y en base a esto, programar actividades futuras de cooperación.

Pedro D'Argenio y Carlos Luna realizarán una visita de trabajo con el propósito de estudiar la integración de herramientas de Model Checking con asistentes de pruebas para la verificación de propiedades de seguridad en el contexto de la tecnología JavaCard.

Otros:

Workshop en Montevideo Noviembre 2001

En oportunidad de la visita de Marieke Huisman a Montevideo se realizará una reunión de trabajo en la que participarán, además de Marieke Huisman, investigadores de los equipos uruguayo y argentino. Se invitará a este workshop a otros investigadores de la región, en particular, de Chile y Brasil.

5 Recursos solicitados y contraparte del Cono Sur

La siguiente tabla justifica los recursos que se solicitan y detalla la contraparte que afrontarán los Grupos de Métodos Formales del InCo y de FaMAF. Todas las cifras están en Francos Franceses.

Motivo	Recursos Solicitados	Contraparte
Visita de Marieke Huisman	10.000	7.000
Workshop	10.000	5.000
Visita de Alberto Pardo	3.500	7.000
Pasantía de Daniel Perovich	40.000	7.000
Visita de Daniel Fridlender	10.000	7.000
Visita de Pedro D'Argenio	10.000	7.000
Visita de Carlos Luna	8.000	7.000
Totales	91.500	47.000

Además de los gastos mencionados en la tabla, los equipos uruguayo y argentino pondrán a disposición del proyecto la siguiente infraestructura informática: 6 estaciones de trabajo, 1 kit de desarrollo para programación JavaCard Cyberflex y un GemExpresso.

Los integrantes de los equipos dedicarán al proyecto los siguientes porcentajes de su tiempo. La última columna detalla la correspondiente fracción del sueldo del integrante en Francos Franceses.

Integrante	Porcentaje	Fracción de sueldo
Javier Blanco	20%	1.500 / mes
Pedro D'Argenio	30%	1.500 / mes
Daniel Fridlender	50%	3.000 / mes
Alberto Pardo	50%	3.000 / mes
Carlos Luna	40%	1.800 / mes
Daniel Perovich	100%	1.000 / mes
Total		11.800 / mes
Total (Sept. 2001 - Marzo 2002)	7 meses	82.600