AT - Annexe Technique
Description technique des travaux de R&D

Nom du projet :	Securité JavaCard
Entreprise ou organisme :	SERMA Technologies / LaBRI

A - Présentation générale du projet

1. Objectifs et finalités du projet

Résultats visés

Intérêt

Ce projet est centré sur l'analyse de la sécurité de la nouvelle génération de cartes à puce JavaCard (sous-ensemble dérivé de Java). Il a pour but de mettre au point une expertise en défauts de sécurité logiciels sur ces produits.

Il s'agit de développer une bonne expertise de la structure des produits répondant aux spécifications JavaCard, afin de pouvoir mettre en œuvre une gamme étendue d'attaques logicielles de haut niveau technique permettant de tester et de valider la qualité de l'implémentation des produits sécurisés soumis à une évaluation Critères Communs ou ITSEC.

Objectifs pour les partenaires

L'intérêt technique de ce projet est d'aboutir à une analyse en profondeur de la sécurité des produits JavaCard développés par les industriels de la carte à puce (ex : Gemplus, Oberthur Card Systems, Schlumberger, Bull) afin d'accompagner leur développement.

Pour le CESTI de SERMA Technologies, ce projet répond à la demande croissante de ces industriels pour l'évaluation sécuritaire de cette nouvelle gamme de produits. L'objectif principal de SERMA Technologies est de pouvoir traiter ce type d'évaluation à l'état de l'art de la recherche logicielle afin de garantir au mieux la pertinence des activités d'évaluation.

Pour le LaBRI les objectifs sont les suivants :

- Transférer ses compétences vers un cadre industriel réel. Ceci se concrétise par les deux points suivants :
  - Exploiter et faire profiter le tissu industriel de la compétence Java dont il dispose;
  - Exploiter une compétence acquise dans la modélisation pour des domaines

très variés, mais aussi plus récemment dans la technologie Java.

- Profiter de cas industriels réels pour :
  - Accroître sa compétence dans le domaine de la technologie Java pour l'embarqué et en particulier les cartes à puce ;
  - S'ouvrir à de nouveaux problèmes concrets qui donneront l'opportunité au LaBRI de concevoir puis mettre en œuvre des solutions complexes ouvrant éventuellement de nouvelles voies de recherche;
- Contribuer le cas échéant à l'évolution des technologies Java et JavaCard en guidant par ces efforts les points clefs à considérer dans les futures spécifications.

Retombées industrielles, économiques et en terme d'emplois, envisageables, d'une part, pour les partenaires du projet et, d'autre part, pour l'ensemble de la société.

Valorisation pour les partenaires

Pour SERMA Technologies, les objectifs principaux de valorisation de ce projet sont les suivants :

- qualité des prestations offertes par le CESTI : des attaques logicielles sophistiquées sur les programmes JavaCard permettront d'évaluer plus efficacement les produits basés sur cette technologie, et de contribuer au développement du marché.

- notoriété : ces nouveaux types de tests renforceront de manière significative le champ des compétences logicielles du CESTI, assurant ainsi la notoriété et la réputation de compétence technique du CESTI de SERMA Technologies.

Pour le Labri, les objectifs sont les suivants :

- Référence du LaBRI vis à vis du monde JavaCard pour la vérification de ce type de technologie;

- Reconnaissance classique d'un laboratoire universitaire à travers des publications;

- Utilisation de ce savoir-faire dans des projets de développement, de conseil ou de mise en place de nouveaux enseignements ;

Intérêt du projet pour les pouvoirs publics

Programme « Société de l'Information » :

Ce projet s'inscrit dans le cadre d'une participation à l'évolution des produits du marché vers une société de l'information. En effet, les produits visés ouvrent de nouvelles possibilités en termes de fonctionnalités et de sécurité (produits multi-applications bancaires, porte-monnaie électronique, signature électronique, …), qui

permettront la mise en place de services tels que le commerce électronique sur Internet sécurisé.

Industrie de la carte :

L'industrie de la carte à puce prévoit un fort développement du marché des produits JavaCard dans les années à venir. Toutefois, la plupart des clients des industriels requièrent aujourd'hui un niveau d'assurance élevé pour la sécurité de ces produits. Pour pouvoir garantir ce niveau de sécurité, les Centres d'Evaluation de la Sécurité des Systèmes d'Information (CESTI) doivent acquérir l'expertise nécessaire.

Protection de la vie privée et de la propriété intellectuelle :

Les évaluations sécuritaires effectuées par des CESTI permettent :

- d'une part, de réaliser une analyse complète de produit au niveau sécuritaire dans un cadre contrôlé garantissant aux industriels la protection de leur propriété intellectuelle, voire la confidentialité de l'évaluation elle-même.

- d'autre part, de garantir aux clients des industriels de la carte que les produits mis sur le marché possèdent un niveau de sécurité éprouvé en fonction de Critères stables et clairement définis, qui protègeront notamment la confidentialité de toute information personnelle et/ou confidentielle des utilisateurs finaux.

Schéma d'évaluation français :

De plus, au niveau national et international, le schéma d'évaluation français, représenté par le DCSSI qui contrôle l'ensemble des Centres d'évaluation, bénéficiera d'une reconnaissance plus forte lorsqu'un des CESTI agréés disposera d'une compétence pointue pour l'évaluation de la sécurité de ce domaine technologique.

Impact économique direct du projet :

La possibilité de valider la sécurité des technologies JavaCard va lever le verrou technologique à son utilisation élargie et permettra un développement plus rapide de la carte à puce.

2. Enjeux techniques et économiques du projet

Description de l'état de l'art et positionnement du projet dans cet environnement;

Etat de l'art

Le marché du logiciel pour cartes à puce se répartit de la façon suivante :

Multos : 50 % du marché, avec une très forte présence dans le domaine bancaire, et particulièrement chez les banques dites vertes. Ce sont des systèmes fermés pour lesquels aucun chargement d'applicatif ne peut intervenir au cours de la vie du produit

JavaCard : 50 % du marché. Il est aussi présent dans domaine du GSM et chez les banques dites bleues. L'avantage est d'avoir un système qui est ouvert c'est à dire sur lequel de nouvelles applications peuvent être mises en place. La contrepartie de cette souplesse est la crainte que l'ajout d'une nouvelle "applet" puisse exposer le produit à des attaques non prévues au départ. Le principal verrou technologique au développement de ce logiciel est ce problème de sécurité. D'où l'intérêt de notre projet de recherche.

Autres : Smartcard pour Windows et Ocapi.

Standards utilisés dans l'environnement JavaCard

Les produits JavaCard actuels soumis à évaluation sont généralement basés sur les spécifications suivantes :

Sun Microsystems :

- JavaCard™ 2.1 Virtual Machine Specification - 1999,
- JavaCard™ 2.1 Runtime Environment (JCRE) Specification - 1999,
- JavaCard Applet Developer's Guide – JavaCard Version 2.1 – August 1999,

Visa International :

- Global Platform - Open Platform – Card Specification Version 2.0.1 – April 2000,

Caractère innovant du projet

Nous avons choisi de réaliser en priorité un travail de recherche sur la sécurité de JavaCard car à ce jour la lecture des comptes rendus de conférences ou de revues spécialisées montrent très peu d'activité de recherche sur ce sujet. Or l'évolution du marché tend à prouver qu'une très large demande devrait se confirmer dans les prochaines années.

Marché visé, qualitativement et quantitativement;

Pour SERMA Technologies, l'essentiel du marché visé aujourd'hui au travers de la réalisation de ce projet concerne les principaux fabricants de cartes à puce et développeurs de « masques » (systèmes d'exploitation pour cartes à puces) tels que :

- Gemplus (leader mondial de la carte à puce),
- Oberthur Card Systems,
- Schlumberger,
- Bull,
- SAGEM,
- Etc…

Ainsi que les fondeurs de silicium comme :

- ST Microelectronics,
- Philips,
- Infineon,
- Atmel,
- Samsung,
- Etc…

Chacun de ces acteurs développe actuellement dans le domaine JavaCard et met sur le marché une à deux plate-formes par an, ainsi que des bouquets d'applets associés.

3. Organisation du partenariat

Présentation générale de SERMA Technologies

SERMA Technologies est une société de Services et d'Ingénierie Technologique spécialisée dans le contrôle des composants, systèmes, cartes électroniques et des matériaux. La branche électronique est répartie sur les sites de Pessac (siège social), Toulouse, Saint-Egrève et Stuttgart (Allemagne), et représente 120 ingénieurs et techniciens.

Le CESTI (Centre d'Evaluation pour la Sécurité des Technologies de l'Information) est un département de la branche électronique de SERMA Technologies.

Le CESTI, comme tous les centres d'évaluation, est supervisé par l'Organisme de Certification français (DCSSI : Direction Centrale pour la Sécurité des Systèmes d'Information), et réalise des évaluations sécuritaires selon les Critères Communs et les ITSEC, ainsi que des expertises sécurité sur des composants électroniques.

Siège social : 30 Avenue Gustave Eiffel – 33608 PESSAC Cedex

Tél : 05 57 26 08 88 – **Fax :** 05 57 26 08 98

Web : http://www.serma.com

Contact responsable du projet : Jean-Pierre LACOUSTILLE - Ingénieur Evaluateur Sécurité

Motivation pour la participation du LaBRI au projet

Partenaire universitaire : LaBRI

Le LaBRI (Laboratoire Bordelais de Recherche en Informatique) est une Unité Mixte de Recherche (UMR 5800) du CNRS (Département des Sciences pour l'Ingénieur) rattachée à l'Université Bordeaux 1 et à l'ENSEIRB.

Ce laboratoire regroupe des chercheurs du CNRS, des enseignants-chercheurs de l'UFR Mathématiques et Informatique et de l'IUT de l'Université Bordeaux 1, de l'ENSEIRB, ainsi que des enseignants-chercheurs de l'Université Montesquieu (Bordeaux 4: Droit et Sciences Economiques) et de l'Université Victor Ségalen (Bordeaux 2 : Médecine et Sciences de la Vie), dont les activités de recherche justifient leur intégration au LaBRI.

Les chercheurs du LaBRI sont répartis en cinq équipes :

- Combinatoire et algorithmique

- Logiques, langages et applications

- Modélisation, vérification et test de systèmes informatisés

- Calcul parallèle et distribué

- Image et son

Adresse : LaBRI, Université Bordeaux I

351 Cours de la Libération – 33406 TALENCE

Rattaché à : Université Bordeaux I – ENSEIRB – CNRS

Tél : 05 56 84 69 00 – **Fax** : 05 56 84 66 69

Web : http://labri.u-bordeaux.fr

Contact responsable du projet : Serge CHAUMETTE – Maître de Conférences

Le choix du LaBRI pour Serma Technologies s'est justifié par trois raisons majeures

Une première expérience avait été menée avec eux un an auparavant sur une formation aux logiciels Java. Nous avions eu l'occasion d'apprécier leurs compétences, et il s'en est suivi une coopération informelle qui nous a permis de développer des tests d'attaque pertinents et reconnus par la suite par le DCSSI.

Le LaBRI est un des laboratoires universitaires français les plus actifs dans le transfert de technologies vers le milieu industriel comme le prouve la mise en place de sa structure dédiée : LaBRI Transfert.

Ce laboratoire est situé à quelques kilomètres de Serma Technologies et le mode de fonctionnement en sera certainement facilité.

Rôle du LaBRI dans le projet;

Le LaBRI apportera sa connaissance approfondie du langage Java, celui-ci étant utilisé au LaBRI depuis plusieurs années dans des applications telles que les systèmes distribués.

L'objectif est d'appliquer cette expérience de Java au langage JavaCard et ainsi de parvenir à identifier ses faiblesses potentielles. Cette approche est justifiée par la plus grande antériorité de Java par rapport à JavaCard qui n'a que quelques années d'existence.

Le LaBRI apportera aussi sa forte compétence en spécifications formelles, indispensable à la modélisation de la spécification JavaCard.

Management et pilotage du projet par SERMA Technologies

L'activité même du CESTI de SERMA Technologies requiert une veille technologique importante afin de rester de façon permanente à l'état de l'art des nouvelles techniques d'expertise et d'attaque de composants électroniques et des logiciels embarqués. C'est pourquoi dans un but d'amélioration des services fournis, SERMA Technologies investit dans la recherche sur les produits JavaCard, pour lesquels un très fort développement est prévu dans les années qui viennent.

4. Description des travaux à mener

Acquis technologiques servant de base au projet

Depuis l'année 1999, le CESTI de SERMA Technologies a eu à réaliser des évaluations sécuritaires de niveau faible (EAL1) sur des produits de type JavaCard. Dans ce cadre, afin de développer les compétences nécessaires, une première expérience a été menée avec le LaBRI sous la forme d'une formation aux logiciels Java ainsi qu'une courte collaboration pour le développement de nouveaux types d'attaques.

Ce premier contact a permis de mettre sur pied une collaboration à plus long terme dans le domaine de JavaCard.

Au niveau technique, le projet se basera sur l'ensemble des spécifications JavaCard existantes qui sont utilisées aujourd'hui par les fabricants de cartes à puce.

Travaux complémentaires nécessaires

Les étapes suivantes sont aujourd'hui prévues pour le développement d'une expertise du système JavaCard et la mise en œuvre de cette expertise pour le montage d'attaques logicielles :

Etape 0 : Prise en main de l'outil JavaCard par le LaBRI et Serma Technologies

Afin de permettre un déroulement efficace du projet, la réalisation d'un certain nombre d'étapes préliminaires est indispensable. Elles sont essentiellement au nombre de trois :

- Collecte de la documentation nécessaire à la compréhension de l'environnement de travail ;
- Etude de la spécification, de l'API et des outils logiciels et matériels associés ;
- Elaboration d'un cas test qui permettra aux partenaires de travailler tout au long du projet et de communiquer tout en se préservant du problème de confidentialité que poserait l'utilisation d'exemples issus de produits effectivement amenés à être mis sur le marché par les clients de Serma.

Etape 1 : Choix d'un microcontrôleur

Serma Technologies sélectionnera un microcontrôleur représentatif des applications pour cartes à puce muni d'un OS générique permettant le chargement en E²PROM d'un soft mask. Il sera ainsi possible d'embarquer la machine virtuelle développée par le LaBRI (si la faisabilité de l'étape 2 est confirmée) et les API.

Etape 2 : Etude et développement d'une machine virtuelle

Du fait de la confidentialité des produits sur lesquels nous serons amenés à travailler, il sera difficile à Serma Technologies de transmettre au LaBRI un produit développé par un de ses clients. En conséquence, le LaBRI étudiera la possibilité (cette hypothèse nécessite une évaluation en termes de moyens humains et techniques) de développer sa propre machine virtuelle ou d'utiliser une machine virtuelle du domaine public accessible avec ses sources selon les mêmes spécifications que les produits de nos clients.

Etape 3 : Analyse de la machine virtuelle JavaCard :

Les applications développées en JavaCard sont compilées et converties en un code interprétable appelé « bytecode ». La Machine Virtuelle (JVM), développée en langage natif, est le moteur d'exécution de ce bytecode. Pour chaque octet de bytecode, la routine correspondante s'exécute. La Machine Virtuelle permet de vérifier dynamiquement certains aspects de la sémantique du bytecode exécuté.

Une analyse approfondie de la structure et du fonctionnement de la Machine Virtuelle permettra de mettre en évidence les aspects sécuritaires non couverts au niveau

sémantique, et les éventuels défauts de sécurité pouvant directement compromettre l'intégrité et la confidentialité du système et des applications (code, données, clés secrètes, …).

Etape 4 : Elaboration d'un modèle partiel ou complet de JavaCard / Spécification formelle

La spécification de la machine Virtuelle JavaCard est pour l'essentiel exprimée en langage naturel, ce qui, de façon classique, laisse une place importante aux ambiguïtés et rend caduques des recherches systématiques de propriétés relatives au fonctionnement du système ainsi décrit.

L'objectif de cette phase du projet est de mettre en place un modèle formel de cette spécification informelle en se basant sur la compétence du LaBRI dans le domaine Java et dans celui de la spécification formelle.

En modélisant de la sorte tout ou partie de la machine JavaCard et des ses APIs, nous espérons être capables d'utiliser un certain nombre d'outils méthodologiques et/ou automatiques nous permettant de valider certaines propriétés du système. Ainsi nous pourrons satisfaire notre objectif qui est de rechercher, de mettre en évidence, et d'expliquer d'éventuelles failles de sécurité de JavaCard.

Etape 5 : Chargement d'applications agressives

Le langage Java permet une programmation s'appuyant sur la définition d'objets et sur l'utilisation restrictive de ces objets par rapport à leur définition. Un programme en Java n'utilise pas d'adresses mémoire réelles ou relatives ni même de pointeurs contrairement à des langages plus classiques tels que le C ou l'assembleur.

Avant de pouvoir être exécutée, une application développée en Java doit passer par un vérificateur de bytecode (appelé « Verifier ») permettant de valider la sémantique du code.

En JavaCard, la génération actuelle de produits ne permet pas d'embarquer le vérificateur (pour des problèmes d'espace mémoire). Cette partie du projet consiste donc à rechercher les possibilités de mise à profit de l'absence de vérificateur pour charger des applications « agressives » violant les règles de sécurité du système, et permettant d'obtenir un accès aux informations protégées des autres applications embarquées.

Etape 6 : Analyses des futures générations de Javacard dans l' objectif de développer des applications virus

Etant donnée l'évolution rapide de la technologie des semi-conducteurs, les futures générations de microcontrôleurs permettront probablement, par une plus grande taille mémoire, d'éliminer le défaut de sécurité potentiel concernant le vérificateur.

Il s'agira donc, en utilisant un vérificateur, d'essayer de mettre au point des applications « virus » capables de tromper l'outil de vérification et d'atteindre ou d'affecter les données sensibles des applications.

Etape 7 : Communication et commercialisation

Tout au long du projet un certain nombres d'actions de communication seront menées pour promouvoir notre savoir faire par l'intermédiaire de :

- publications,

- participations à des groupes de travail (Java Card forum www.javacardforum.org),

- communications dans des conférences telles que Eurosmart (juin 2001 Marseille), Card 2001 (Octobre Paris), autres conférences…

Actions envisagées par les partenaires pour assurer une reproductibilité à plus grande échelle de l'étape d'expérimentation.

Au terme du projet, les partenaires prévoient de formaliser les attaques développées sous forme d'un « jeu d'applets agressives » permettant de tester la résistance de divers produits basés sur JavaCard à des attaques similaires.

En fonction des faiblesses qui auront pu être identifiées, des procédures de vérification systématique de certaines caractéristiques des produits pourront être établies, en collaboration avec la DCSSI (Direction Centrale pour la Sécurité des Systèmes d'Information).

Démarche envisagée vis à vis de l'évaluation et de la certification de la sécurité des technologies de l'information.

La démarche de ce projet s'inscrit exactement dans le cadre de l'évaluation et de la certification de la sécurité des technologies de l'information, puisque le CESTI de SERMA Technologies est agréé depuis plus de 6 mois pour réaliser des évaluations sécuritaires de haut niveau.

La réussite du projet contribuera à améliorer la position du schéma français d'évaluation et de certification (représenté par la DCSSI) au niveau national et international, qui bénéficiera d'une reconnaissance plus forte lorsqu'un des CESTI agréés disposera d'une compétence pointue reconnue par les industriels pour l'évaluation de la sécurité de ce domaine technologique.

5. Déroulement du projet

Phase 1 (5 mois) : Etapes 0, 1 et 2 décrites précédemment

Durant cette phase, il s'agira de prendre en main et de développer les outils nécessaires aux travaux de recherches ultérieurs.

Phase 2 (5 mois) : Etapes 3 et 4

Dans cette phase l'analyse de la machine virtuelle JavaCard permettra d'en élaborer un modèle afin de valider les propriétés du système.

Phase 3 (5 mois) : Etapes 5, 6 et 7

Cette phase consistera à développer des tests d'attaque sur les produits actuels et sur les futures générations de produits.

Planning : le tableau ci-dessous dresse le planning prévisionnel du déroulement des phases du projet, incluant la fourniture de rapports d'activités au terme de chaque phase.

Phases du projet / Mois	**01/01**	**02/01**	**03/01**	**04/01**	**05/01**
Phase 1 : Prise en main et développement des outils nécessaires					
Etape 0 : Prise en main de l'outil JavaCard					
Etape 1 : Sélection d'un microcontrôleur	SERMA : fourniture d'un produit permettant de charger une VM JavaCard				
Etape 2 : Etude et développement d'une VM JavaCard		LaBRI : résultats de l'étude de la VM ou VM développée			
Rédaction et livraison d'un rapport d'activités intermédiaire (R.I.1) pour la phase 1					LaBRI + SERMA : R.I.1

Phases du projet / Mois	**06/01**	**07/01**	**08/01**	**09/01**	**10/01**
Phase 2 : Modélisation					
Etape 3 : Analyse de la VM JavaCard	LaBRI + SERMA : premiers tests sur échantillons				
Etape 4 : Modélisation de JavaCard / Spécification formelle			LaBRI : modèle formel de JavaCard		
Rédaction et livraison du rapport d'activités intermédiaire (R.I.2) pour la phase 2					LaBRI + SERMA : R.I.2

Phases du projet / Mois	11/01	12/01	01/02	02/02	03/02
Phase 3 : Développement d'attaques logicielles					
Etape 5 : Développement et chargement d'applications agressives	SERMA + LaBRI : jeu d'applications agressives de premier niveau (pas de Verifier embarqué)				
Etape 6 : Nouvelles générations de produits : attaques par applications « virus »				SERMA + LaBRI : jeu d'applications « virus » ou de deuxième niveau (Verifier embarqué)	
Etape 7 : Communication et commercialisation					
Synthèse : rédaction par les partenaires d'un rapport final complet (R.F) des travaux effectués					LaBRI + SERMA : R.F.

Les rapports intermédiaires synthétiseront les activités menées au cours des étapes principales de la phase en cours ainsi que les résultats obtenus.

Des réunions de suivi pourront également être planifiées en fin de phases afin de présenter les travaux effectués. Un intervenant de la DCSSI pourra être convié à ces réunions afin de suivre l'avancement du projet.

B - Description des travaux de R&D

Positionnement de ces travaux dans l'activité du partenaire (état du projet, résultats déjà acquis, études de faisabilité, liaison avec d'autres projets,…)

Le LaBRI dispose déjà d'une forte compétence en terme de technologie Java et de modélisation aussi bien dans le domaine de Java que dans d'autres types de systèmes et de technologies. En particulier des travaux récents sur la modélisation du système de threads Java (thèse de Asier Ugarte) ont permis de toucher du doigt la difficulté de la problématique, mais dans le même temps d'acquérir une expérience qui sera exploitée dans le cadre de cette collaboration.

Afin d'amorcer le projet, le LaBRI a commencé à étudier les spécifications JavaCard dans le cadre d'un mémoire de DEA.

En ce qui concerne SERMA Technologies, ce projet se situe parmi plusieurs axes de recherche identifiés à ce jour :

- Développement d'attaques physiques, intrusives ou non, dont l'objectif est d'atteindre les biens à protéger,
- Attaques par analyse et traitement des signaux électriques et électromagnétiques,
- Développement d'attaques logicielles à ce jour principalement sur JavaCard,

L'objectif de ces travaux est de pouvoir maîtriser la globalité des compétences nécessaires à l'évaluation de cartes à puce, quel que soit le domaine d'application (bancaire, transport, santé, GSM, internet, …).

Description des développements à effectuer et difficultés particulières à résoudre

Les développements prévus dans le cadre de ce projet sont décrits de manière détaillée dans le chapitre 4 ci-dessus (cf. « Travaux complémentaires nécessaires »).

Pour les partenaires, les difficultés principales en termes de R&D porteront d'une part sur le passage de la spécification informelle de JavaCard à un modèle effectivement exploitable et d'autre part sur l'étude de faisabilité (et de la réalisation éventuelle) d'une machine virtuelle JavaCard dans le cadre des moyens impartis.