Nom du projet :	Sécurité Java Card
Entreprises ou organismes :	SERMA Technologies / LaBRI

Projet Sécurité Java Card

Rapport d'avancement
Phase 1
Juin 2001 à Octobre 2001

Serge Chaumette, LaBRI
Jean-Pierre Lacoustille, SERMA
Damien Sauveron, SERMA/LaBRI

Résumé

La technologie Java Card occupe 50 % du marché du logiciel pour cartes à puce multi-applicatives, les 50 % restants étant occupés par Multos. A ce jour, cette technologie est surtout utilisée dans le domaine bancaire et dans le domaine du GSM. Son avantage est d'offrir un système ouvert, c'est à dire un système sur lequel de nouvelles applications peuvent être mises en place, soit les applications résidentes peuvent être mises à jour. La contrepartie de cette souplesse est le risque que l'ajout d'une nouvelle "applet" puisse exposer le produit à des attaques non envisagées au départ. Ce problème de sécurité est le principal obstacle au développement de cette technologie.

C'est dans ce cadre que SERMA Technologies et le LaBRI réalisent en commun le projet intitulé « Sécurité Java Card ». Ce rapport intermédiaire en rappelle le contenu et synthétise les activités menées au cours de sa première phase ainsi que les résultats obtenus.

Nom du projet :	Sécurité Java Card
Entreprises ou organismes :	SERMA Technologies / LaBRI

1 Présentation générale du projet - Rappel

1.1 Objectifs et finalités

L'industrie de la carte à puce prévoit un fort développement du marché des produits Java Card 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 Technologies de l'Information (CESTI) doivent acquérir l'expertise nécessaire.

C' est ainsi que 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 Java Card. Dans ce cadre, afin de développer les compétences nécessaires, une première expérience a été menée avec le LaBRI sous la forme d'une formation au langage 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 Java Card.

Cette collaboration est centrée sur l'analyse de la sécurité de la nouvelle génération de cartes à puce Java Card (sous-ensemble dérivé de Java). Elle 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 Java Card, 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.

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 Java Card 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).

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 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, puisqu' il bénéficiera naturellement 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.

1.2 Partenaires

Partenaire industriel : SERMA Technologies

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

L'activité même du CESTI de SERMA Technologies requiert une veille technologique importante afin de rester de façon permanente à la pointe 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 Java Card, pour lesquels un très fort développement est prévu dans les années qui viennent.

Partenaire universitaire : LaBRI

Le LaBRI (Laboratoire Bordelais de Recherche en Informatique) est une Unité Mixte de Recherche (UMR 5800) du CNRS (Département STIC, anciennement SPI) 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 1

351 Cours de la Libération – 33405 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 LaBRI apporte sa connaissance approfondie du langage Java, celui-ci étant utilisé au sein du laboratoire depuis plusieurs années dans des applications telles que les systèmes distribués. L'objectif est d'appliquer cette expérience de Java à la technologie Java Card et ainsi de parvenir à identifier ses faiblesses potentielles. Cette approche est justifiée par la plus grande antériorité de Java par rapport à Java Card qui n'a que quelques années d'existence. Le LaBRI apporte aussi sa forte compétence en spécifications formelles, indispensable à la modélisation de la spécification Java Card.

2 Programme de déroulement du projet et état actuel

2.1 Rappel du programme de déroulement du projet

Nous rappelons ici le programme initial du projet.

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

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

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

Etape 0 : Prise en main de l'outil Java Card par le LaBRI et SERMA Technologies
Etape 1 : Choix d'un microcontrôleur
Etape 2 : Etude et développement d'une machine virtuelle

Phase 2 (5 mois) : Etapes 3 et 4

Dans cette phase l'analyse de la machine virtuelle Java Card doit permettre d'en élaborer un modèle afin de valider les propriétés du système.

Etape 3 : Analyse de la machine virtuelle Java Card
Etape 4 : Elaboration d'un modèle partiel ou complet de Java Card / Spécification formelle

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

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

Etape 5 : Chargement d'applications agressives
Etape 6 : Analyses des futures générations de Java Card dans l' objectif de développer des applications virus.
Etape 7 : Communication et commercialisation

2.2 Bilan de la phase 1

Comme décrit dans le projet initial, l' objectif était de prendre en main et de développer les outils nécessaires aux travaux de recherche ultérieurs. Nous dressons ici un bilan des travaux réalisés, nous justifions les choix effectués et les modifications éventuelles qui en découlent.

Etape 0 : Prise en main de l'outil Java Card par le LaBRI et SERMA Technologies

Afin de permettre un déroulement efficace du projet, la réalisation d'un certain nombre d'étapes préliminaires était 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 permette 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.

La collecte de la documentation a été amorcée dans le cadre :

- *du mémoire de DEA de Damien Sauveron* : Sécurité et vérification d'applications embarquées en environnement Java Card.

- *d'un rapport interne au LaBRI (RR-1259-01) de Damien Sauveron :* La technologie Java Card : Présentation de la carte à puce. La Java Card.

Damien Sauveron a été recruté sur une bourse CIFRE à compter du 1er septembre 2001. Il a ainsi travaillé sur l' étude de la spécification et a pris en main les outils

associés, afin de conseiller le LaBRI dans l'achat d'une plate-forme de développement pour cartes à puces Java. Le choix s'est porté sur le kit de développement de Gemplus (GemXpresso RAD 211 PK).

L'élaboration d'un cas test a été réalisée. L'application choisie est un porte-monnaie électronique développé à partir de la spécification CEPS (Common Electronic Purse Specification), en version simplifiée afin de conserver une taille de code raisonnable.

Etape 1 : Choix d'un microcontrôleur

Dans cette étape il était convenu que SERMA Technologies sélectionnerait un microcontrôleur représentatif des applications pour cartes à puce muni d'un OS générique permettant le chargement en E²PROM d'un soft mask. Il devait ainsi être possible d'embarquer la machine virtuelle développée par le LaBRI (si la faisabilité de l'étape 2 était confirmée) et les API.

Plutôt que de cibler un microcontrôleur, nous avons finalement décidé de réaliser un émulateur sur PC. Parmi les avantages qui ont conduit à ce choix, ceci nous permettra de travailler virtuellement sur les plate-formes et les microcontrôleurs des différents constructeurs par un paramétrage approprié de notre émulateur. L'idée initiale de ce microcontrôleur se traduit maintenant en contraintes sur la machine virtuelle qui va être développée : elle devra reproduire le plus fidèlement possible les conditions effectives de fonctionnement d'une machine Java dans une carte à puce (limitation mémoire, etc…). De plus, il est toujours plus facile d'intégrer des outils de collecte de traces ainsi que d'autres mécanismes (nécessaires et utiles dans un environnement logiciel) que dans du matériel. Nous pourrons ainsi fournir avec notre émulateur des outils de haut niveau facilitant la mise en œuvre d'attaques et leur observation afin de concourir au mieux à la réalisation du projet.

Etape 2 : Etude et développement d'une machine virtuelle

Du fait de la confidentialité des produits sur lesquels SERMA Technologies est amenée à travailler, il lui est difficile de transmettre au LaBRI un produit développé par un de ses clients. En conséquence, le LaBRI doit étudier 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.

Même si l'étude de ce point a déjà commencé, cette étape a été décalée du fait que le recrutement de l'ingénieur prévu dans le cadre du financement du LaBRI n'a naturellement pas pu être déclenché avant la notification effective des crédits au responsable scientifique. Ce recrutement est aujourd'hui en cours.

3 Plannings

3.1 Planning prévisionnel

Le tableau ci-dessous reprend 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 Java Card					
Etape 1 : Sélection d'un microcontrôleur	SERMA : fourniture d'un produit permettant de charger une VM Java Card				
Etape 2 : Etude et développement d'une VM Java Card		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 Java Card	LaBRI + SERMA : premiers tests sur échantillons				
Etape 4 : Modélisation de Java Card / Spécification formelle			LaBRI : modèle formel de Java Card		
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.

3.2 Planning révisé

Du fait des décalages dans l'évaluation des propositions et donc des avis émis, on peut considérer que le projet a effectivement débuté mi-juin 2001. Ceci conduit à un décalage de l'ensemble du projet.

De plus la notification de crédits arrivée à l'Université Bordeaux 1 en septembre n'a pas permis de lancer le recrutement de l'ingénieur devant participer au projet dans le temps prévu. Ceci conduit à un décalage de l'étape 2 de la phase 1. Ainsi cette étape est décalée sur la phase 2.

Phases du projet / Mois	**06/01**	**07/01**	**08/01**	**09/01**	**10/01**
Phase 1 : Prise en main et développement des outils nécessaires					
Etape 0 : Prise en main de l'outil Java Card	Collecte de la documentation nécessaire (fin DEA Damien SAUVERON)			Prise en main des outils Java Card	
Etape 1 : Sélection d'un microcontrôleur		Décision de travailler sur un environnement d'émulation sur PC.			
Etape 2 : Etude et développement d'une VM Java Card		LaBRI : Etude démarrée – Recrutement ingénieur développement en cours			
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	**11/01**	**12/01**	**01/02**	**02/02**	**03/02**
Phase 2 : Modélisation					
Etape 2 : Etude et développement d'une VM Java Card	LaBRI : développement VM				
Etape 3 : Analyse de la VM Java Card	Analyse pour modélisation				
Etape 4 : Modélisation de Java Card / Spécification formelle			LaBRI : modèle formel de Java Card		
Rédaction et livraison du rapport d'activités intermédiaire (R.I.2) pour la phase 2					LaBRI + SERMA : R.I.2

Le planning de la phase 3 n'est pour l'instant pas modifié mais simplement décalé, de 5 mois et demi.

Phases du projet / Mois	**04/02**	**05/02**	**06/02**	**07/02**	**08/02**
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.

Etant donné le décalage important constaté, il conviendra de faire une demande officielle de modification de calendrier avant la fin du projet.

4 Conclusion

Ce premier rapport permet de recadrer le projet aussi bien en terme de déroulement que de calendrier. De plus, les choix principaux ont maintenant été effectués. Les phases et étapes suivantes devraient se dérouler conformément à la description réalisée dans le présent document.