Projet Sécurité Java Card Collaboration LaBRI / SERMA Technologies

Serge Chaumette
Serge.Chaumette@labri.fr

LaBRI, UMR CNRS 5800
Université Bordeaux 1

Les partenaires

- SERMA Technologies

SERMA TECHNOLOGIES

- LaBRI, équipe SOD

Cadre du projet

- Labellisé Programme Société de l'Information (PROGSI) par le Secrétariat d'État à l'Industrie
  - Cf. présentation suivante de Laurent Perdiolat

Objectifs du projet

- Mettre en place une expertise en défauts de sécurité logiciels sur les cartes à puces Java
- Mettre en œuvre une gamme étendue d'attaques logicielles de haut niveau technique

Objectifs du projet (suite)

- Tester et valider la qualité des implémentations des produits sécurisés
  - Références
    - Critères communs
    - ITSEC
  - Cibles
    - Services
    - Machine Virtuelle Java

Moyens humains

- SERMA Technologies
  - Jean-Pierre Lacoustille
  - Agnés Paillard
- Équipe Systèmes et Objets Distribués du LaBRI
  - Serge Chaumette
  - Alain Griffault (équipe MVTSI)
  - Un ingénieur
    - Iban Hatchondo

Moyens humains (suite)

- Chercheurs Communs
  - Un doctorant CIFRE
    - Damien Sauveron

Équipe SOD
Systèmes et Objets Distribués

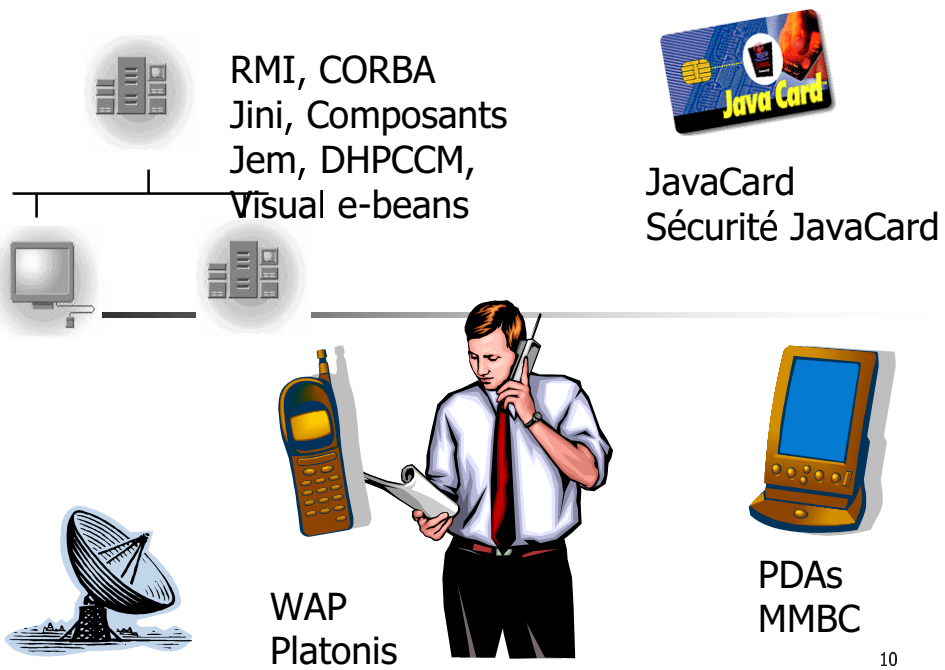
Principal objectif

- L'objectif de l'utilisateur est d'exécuter son application de façon transparente sur la meilleur configuration disponible, i.e. avec un maximum d'efficacité et de sécurité.
- L'objectif du programmeur est de développer son application de la façon la plus simple et la plus sécurisante possible.
- Notre objectif est de contribuer à la conception et au développement d'outils et d'environnements d'exécution formellement validés, permettant de répondre à ces attentes.

Équipe SOD
Actions de recherche

- Aide à la distribution automatique de codes Java *multi-threadés*
- Supports d'exécution distribués
- Validation formelle et pratique de systèmes
- Java embarqué et non filaire, cartes à puce, *nomadique*
- ...

Serge.Chaumette@labri.fr



Méthodologie du projet Sécurité Java Card

- Développer une expertise
  - Java et cartes à puce
- Attaques concrètes
- Environnement de test
  - Emulateur
- Modélisation
  - SOD + MVTSI

Exemple de résultat concret

- Le contenu précis des travaux menés avec SERMA étant confidentiels, l'exemple suivant se situe dans le cadre plus général du langage Java mais illustre parfaitement la démarche que nous appliquons pour la Java Card.
- Cet exemple est un des résultats obtenus avec *Asier Ugarte* pendant sa thèse

Illustration dans un cadre Java
Quelques risques

- Le ramasse-miettes
  - Ordonnancement
- Les *threads*
  - Ordonnancement
  - Mémoire partagée
  - Verrous
- Le chargement dynamique
  - Vérification du code

Illustration dans un cadre Java
Exemple

- Problème connu d'accès aux variables 64 bits
  - On y accède sous la forme de deux parties de 32 bits
    - Risque de résultat indéterministe et donc potentiellement faux
- Analogie

Illustration dans un cadre Java
Construction d'un modèle

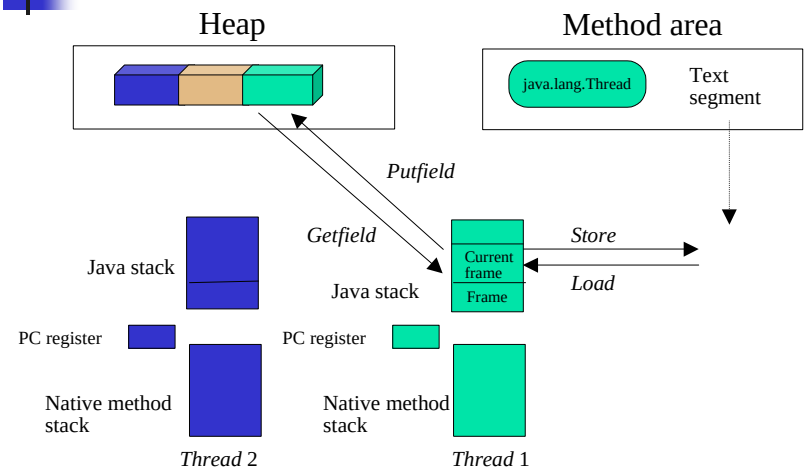


Illustration dans un cadre Java
Construction d'un modèle (suite)

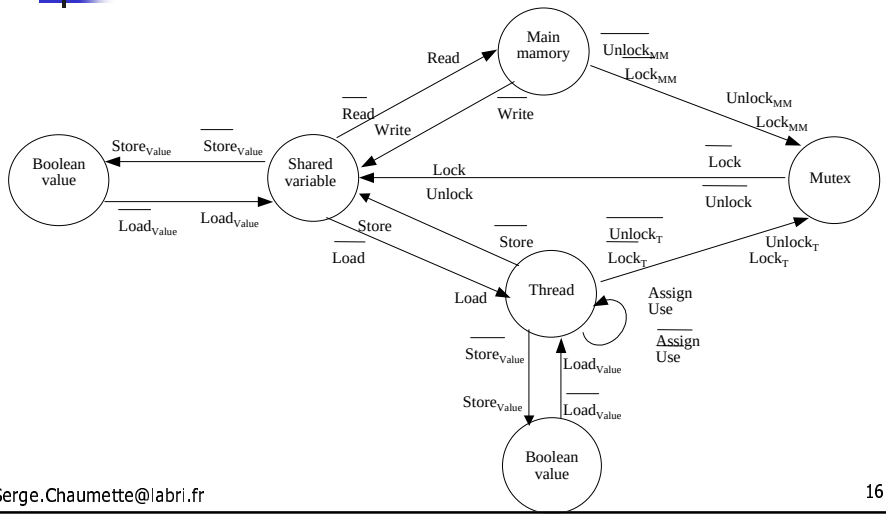


Illustration dans un cadre Java
Construction d'un modèle (suite)

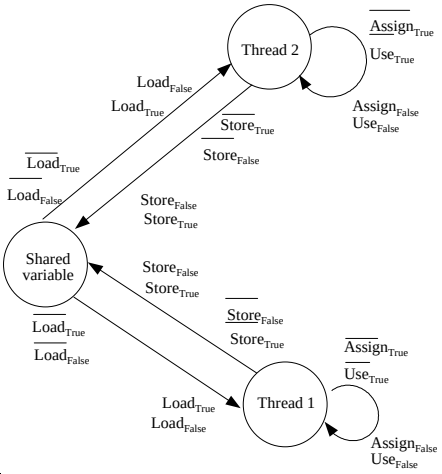
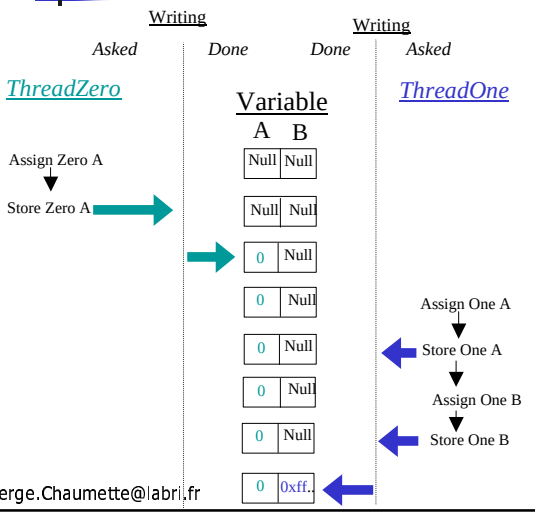


Illustration dans un cadre Java
Liaison avec un programme réel




```
Class Sample{

 long field;

 void setToZero(){
   field = field & 0;
 }

 void  setToOne(){
   field = field | 0xffffffff;
  }
}
```

Illustration dans un cadre Java Résultat

- Preuve que le risque existe effectivement
- On exhibe les conditions dans lesquelles le risque se concrétise

Les bénéfices de la collaboration

- Amélioration du schéma français d'évaluation et de certification représenté par la DCSSI
- Compétence pointue du CESTI de Serma sur les Java Cards
- Pour le LaBRI, transfert, problématiques industrielles, recul sur le langage

A long terme
multiplication des cibles

Serge.Chaumette@labri.fr