SERMA TECHNOLOGIES

CESTI

Evaluer la sécurité des cartes à puce par les Critères Communs

Jean-Pierre LACOUSTILLE - Evaluateur Sécurité

Bordeaux, 19 décembre 2001

Caractéristiques des cartes multi-applicatives

- Capables de gérer des applications de différents types (bancaire, fidélité, transport, etc…) sur la même plate-forme,
- Permettent une mise à jour dynamique du contenu de la carte pendant son cycle de vie (chargement d'applications, nouvelles versions),
- Utilisent généralement une machine virtuelle (ex. JavaCard) pour interpréter les applications écrites dans un langage portable de haut niveau.

Nouveaux problèmes de sécurité

- Une séparation efficace des applications et des "security domains" doit être assurée,
- Le chargement/déchargement d'applications doit être strictement contrôlé,

Objectif : éviter tout accès non autorisé aux données ou au code d'une application

Le standard Critères Communs

Common Criteria for Information Technology Security Evaluation - Norme ISO 15408:1999 (V2.1)

But : évaluer les propriétés de sécurité de produits ou systèmes « IT ».

Principe : définir pour un produit des « Objectifs de Sécurité » permettant de protéger les « biens » identifiés dans l 'environnement d 'utilisation.
Ex : isolation des applications, contrôle d 'accès pour le chargement de nouvelles applications.

L'évaluation permet d 'assurer que le produit remplit ses objectifs de sécurité.

Les niveaux d 'évaluation

Les objectifs de sécurité se traduisent dans les CC par :

- des Exigences Fonctionnelles de Sécurité sur le produit,
- des Exigences dites « d 'Assurance », mesures à prendre par le développeur pour garantir que le produit remplit ses objectifs.

Niveaux d 'évaluation définis par groupement d'exigences d 'assurance en 7 packages appelés EAL1 à EAL7 (Evaluation Assurance Level)

Couverture de l 'évaluation

La couverture, et donc le niveau de connaissance du produit par l 'évaluateur sont croissants en fonction du niveau choisi. Exemples :

Niveau EAL1+ :
- Spécifications fonctionnelles et guides d 'utilisation,
- Tests de pénétration au niveau dit « faible ».

Niveau EAL4+:
- Documentation complète de développement du produit (jusqu 'à l 'implémentation) et de son environnement,
- Tests de pénétration au niveau « Elevé »
- Audit de l 'environnement de développement.

Cahier des charges sécuritaire

Défini dans un document appelé Cible de Sécurité, décrivant :

- les biens, les menaces, les objectifs de sécurité,

- les exigences fonctionnelles et d 'assurance pour le produit,

et identifiant les Fonctions de Sécurité du produit.

La Cible de Sécurité peut être rédigée à partir d 'un cadre prédéfini appelé Profil de Protection.

Profils de Protection

↳ En général rédigés par des groupements d 'industriels.

↳ Expression des exigences fonctionnelles et d 'assurance répondant aux objectifs de sécurité d 'une catégorie de produits.

Quelques exemples :
- Microcontrôleurs : PP/9806 et PP SSVG (Semiconductor & Card Vendors Group).

- Cartes avec applications : PP/9911, PP SCSUG (Smart Card Security User Group)

Le schéma d 'évaluation français

Commanditaire

- Rédige la cible de Sécurité,
- Finance l 'évaluation,
- Fournit les éléments de preuve,
- Reçoit le certificat

CESTI

- Réalise les travaux d 'évaluation selon la méthodologie (CEM)

DCSSI

- Contrôle le processus d 'évaluation,
- Remet le certificat

Les travaux d 'évaluation sont réalisés par un centre indépendant, sous contrôle de la DCSSI.

La reconnaissance mutuelle

Des accords de reconnaissance mutuelle permettent d 'étendre la validité des certificats au niveau international :

- MRA (tous les niveaux EAL) : 13 pays européens.
- SOGIS (jusqu 'au niveau EAL4) : Europe, EU, Canada, Australie, N. Zélande.

Contenu d ’une évaluation CC

En fonction du niveau EAL choisi, le CESTI doit mener à bien les travaux suivants :

- Analyse de la documentation du produit,

- Vérification de la conformité du produit avec les caractéristiques de sécurité annoncées,

- Tests de pénétration : vérification de l ’efficacité des mesures sécuritaires mises en place. « Potentiel d ’attaque » variable en fonction du niveau choisi.

Tests de pénétration sur cartes à puce

Exemples d ’attaques non invasives :

- Test des détecteurs : variations de température, fréquence, ou tension.

- Rayonnements lumineux ou ionisants, application à l ’injection de fautes (DFA).

- Observation du courant Icc (SPA, DPA).

- Attaques logicielles : mise en défaut des mécanismes d ’isolation et d ’intégrité du code et des données des applications embarquées.

Attaques invasives

Quelques attaques invasives :

- Rétro-conception des blocs fonctionnels du microcontrôleur,
- Probing physique pour observation des bus,
- Modification de circuit (par FIB),
- Récupération ou corruption de données.

Les CC et les cartes multi-applicatives

Les CC permettent une approche modulaire pour l 'évaluation des cartes multi-applicatives:

- Possibilité d 'évaluer une plate-forme multi-applicative vierge (sans applications).
- Différentes applications, utilisant les services de sécurité de la plate-forme, peuvent ensuite être certifiées sur cette plate-forme à coûts et délais moindres.

L ’évaluation de cartes multi-applicatives

- Le standard CC est largement reconnu et mis en pratique dans l ’industrie de la carte à puce.
- Les CC sont particulièrement adaptés à la modularité des produits multi-applicatifs.
- Plusieurs produits de type plate-formes multi-applicatives ont déjà été certifiés en France (Gemplus, Oberthur, Schlumberger, …).

CESTI de SERMA - Statut actuel

- Accrédité par le COFRAC depuis février 2000,
- Agréé par la DCSSI depuis juillet 2000 pour le domaine suivant :

« Evaluations CC jusqu’au niveau EAL4+ (potentiel d’attaque “Elevé”) sur des composants ainsi que sur des logiciels embarqués développés en JavaCard. »

CESTI : Quelques réalisations

- Evaluation et maintenance (EAL4+) de la famille ST19SFxx de STMicroelectronics
- Evaluation EAL1+ des plate-formes JavaCard de :

  - GEMPLUS (GemXpresso 211),
  - OBERTHUR CS (Galactic 2.1 V2)
  - SCHLUMBERGER (Palmera Protect V2.0)

- Evaluation EAL1+ carte CT2000 d 'ASK
- Evaluation EAL1+ du composant S3C8975 de SAMSUNG Electronics

Merci de votre attention
&
bonne journée !