EDITE de Paris
École Doctorale Informatique, Télécommunications et Électronique

Progress Report

CEA/CESTI-LETI

Analysis and Research of Points of Interest in the Context of Side-Channel Attacks on Smart Card

Eleonora Cagli
Ph.D Student since 13/10/2014

CEA Grenoble
17 rue des Martyrs
38054 Grenoble Cedex 9

Directeur de Thèse
Emmanuel Prouff
Encadrante
Cécile Dumas

Table des matières

1 Introduction

Contrairement à ce que peut laisser croire son nom au premier abord, les activités de recherche du CEA [1] dépassent de loin les seuls domaines de l'énergie. En plus des énergies bas carbone, les 15 000 employés des 10 centres du CEA étudient en effet la défense et sécurité, les technologies pour la santé et les technologies de l'information. J'ai ainsi eu la chance d'effectuer mon stage dans cette dernière branche, au coeur des 64 hectares du centre grenoblois de 3 000 personnes. Le sujet du stage était en lien avec un dispositif discret mais néanmoins omniprésent : la carte à puce.

1.1 Besoin en sécurité des cartes à puce

La carte à puce est un système embarqué léger inventé en 1974 par Roland Moreno. Elle est employée comme dispositif d'authentification en coordination avec un terminal hors-ligne ou en ligne, et rend des services fonctionnels, comme des retraits ou des crédits bancaires par exemple. Les cartes à puce sont aujourd'hui un élément clé de notre environnement, de par leurs applications multiples : carte de téléphone, de santé, de paiement, de transport, d'accès, ... Elles représentent un médium d'authentification simple, à bas coût et à haut niveau de sécurité. Elles sont donc très utilisées, leur nombre est passé de 540 millions en 2000 à près de 7 milliards en 2012, et devrait atteindre 7,7 milliards pour 2013[**eurosmart:general-assembly:2013**]. Cet effet de masse amplifie les risques associés à la sécurité car chaque vulnérabilité découverte a une très grande cible potentielle. De plus, les cartes sont déployées dans des environnements généralement peu protégés et globalement hostiles. Elles peuvent en effet être volées, des terminaux malveillants peuvent tenter d'accéder aux informations confidentielles qu'elles contiennent, et les porteurs des cartes eux-mêmes ont souvent un intérêt à essayer de percer leurs secrets. La diversité des cas d'utilisation rend leur sécurisation d'autant plus difficile à mettre en œuvre.

1.2 Le CEA CESTI

En réponse à ce besoin de sécurité, l'Etat et les banques imposent aux fabricants de cartes à puce de faire certifier leurs produits avant leur commercialisation, et tout au long du cycle de vie du produit. En France, c'est l'**ANSSI** [2] qui délivre des certificats associés à un **EAL** [3]. Les EAL sont numérotés de 1 à 7, et à chaque niveau d'assurance correspond des exigences de sécurité et de tests différents, le niveau 7 étant le plus exigeant. Ces exigences sont fixées par les Critères Communs [**cc:vol1:31r4** ; **cc:vol2:31r4** ; **cc:vol3:31r4**] qui constituent un standard (ISO/CEI15408) pour la sécurité des systèmes d'information, reconnu par de nombreux états dans le monde, dont l'Europe et les Etats-Unis. Une présentation des Critères Communs et une application à un projet réel sont donnés dans [**stouls:inria-00384217**]. Lorsque le concepteur d'une carte à puce souhaite commercialiser un produit, il doit donc répondre à un ensemble d'exigences fonctionnelles de sécurité, et d'exigences d'assurance de sécurité correspondant à l'EAL visé, avant de demander à un **CESTI** [4], mandaté par l'ANSSI, d'évaluer le système

1. Commissariat à l'énergie atomique et aux énergies alternatives
2. Agence Nationale de la Sécurité des Systèmes d'Information
3. *Evaluation Assurance Level*, ou niveau d'assurance d'évaluation.
4. Centre d'Evaluation des Systèmes et Technologies de l'Information

et ces exigences. Une part significative de cette évaluation consiste en un audit des vulnérabilités du ”composant nu” d’une part (le matériel) et du ”composant masqué” (le logiciel embarqué) d’autre part. À l’issue de cet audit, le CESTI rend un rapport sur lequel l’ANSSI se base pour délivrer la certification du produit. Le CEA de Grenoble comporte un CESTI, le CESTI-LETI, qui est la structure qui m’a accueilli durant le stage.