Divers apports de l'analyse de distributions de la fuite dans les attaques par analyse de canaux auxiliaires

Clavier Christophe, christophe.clavier@unilim.fr
Tél : 0555457398
Tél : 0

Equipe : CRYPTIS, Limoges

Mots clés : cryptologie, cartes à puce, sécurité, analyse de canaux auxiliaires, statistiques

Résumé de la thèse :

Cette thèse concerne la conception de nouvelles attaques et de nouvelles contre-mesures dans le domaine de l'analyse de courant sur des fonctions cryptographiques exécutées par une carte à puce. Plus précisément, il s'agit ici d'étudier l'apport potentiel d'un nouveau type d'exploitation de la consommation de courant : pouvoir distinguer la valeur d'une sous-clé, non pas sur la base de valeurs individuelles d'une donnée intermédiaire d'un calcul, mais sur la base de la distribution statistique de ces valeurs.

This PhD aims at designing new side-channel attacks (power analysis) on cryptographic algorithms, and their related counter-mesures, in the context of smartcard execution of cryptographic functions. More precisely, the goal is to study the potential benefit taken from a new type of exploitation of the power consumtion: being able to distinguish a subkey value, no more from the individual values of an intermediate data of a computation, but rather from the statistical distribution of these values.

Objectifs :

Étudier une façon nouvelle d'appréhender l'exploitation du canal auxiliaire (consommation de courant) dans les attaques par observation sur cartes à puce. Ce nouvel angle de vue est prometteur et pourrait lever certains verrous vis-à-vis de contre-mesures existantes dans les produits actuels.

Description complète du sujet de thèse :

* Introduction

Les cartes à puce sont des composants de sécurité offrant au monde extérieur les fonctionnalités d'authentification, de chiffrement et de signature numérique, autant de services assurés par des fonctions de cryptographie (symétrique ou asymétrique) utilisant des données secrètes - les clés - stockées de manière sécurisée dans la mémoire de la carte. De ce point de vue, on peut dire que la spécificité première d'une carte à puce est d'être un "bunker" à clés cryptographiques (et autres données sensibles).
Malgré la sécurité mathématiquement prouvée (ou au moins éprouvée) des fonctions cryptographiques utilisées, la sécurité concrète des cartes à puce s'est vue menacée à partir de la fin des années 90 avec les publications de nouvelles classes d'attaques que sont l'analyse des canaux auxiliaires et l'analyse de fautes. Nous nous intéresserons pour cette thèse plus particulièrement à l'analyse des canaux auxiliaires dont le principe général est de corréler des

valeurs intermédiaires sensibles de la fonction cryptographique à des grandeurs physiques mesurables comme par exemple la consommation de courant de la carte.

* Sujet de recherche

Bien que les analyses de canaux auxiliaires et les analyses de fautes soient le plus souvent intimement liées à l'algorithme cryptographique dont l'attaquant recherche la clé, elles ne visent pas les fonctions cryptographiques elles-mêmes en tant qu'objet mathématique, mais plutôt l'utilisation effective de ces fonctions, leur implémentation concrète sur un composant électronique.

L'analyse de canaux auxiliaires permet de retrouver des secrets (clés) manipulés lors de l'exécution d'une fonction cryptographique par une carte à puce.
Classiquement, son principe consiste à exploiter la dépendance entre, d'une part une donnée intermédiaire du calcul qui dépend d'une partie de la clé, d'autre part la consommation de courant (ou autre grandeur physique) mesurée lors de la manipulation de cette donnée intermédiaire.

Les méthodes les plus utilisées pour analyser la consommation de courant comprennent :

- l'analyse simple du courant (SPA) qui permet d'obtenir de l'information à partir d'une seule trace et est le plus souvent utilisée en cryptographie asymétrique (exponentiation modulaire RSA par exemple),

- l'analyse différentielle du courant (DPA) et l'analyse du courant par corrélation linéaire (CPA) qui exploitent statistiquement un ensemble de traces de courant (de quelques dizaines à plusieurs milliers) et permettent de définir un test d'hypothèse sur une partie de la clé. Ces attaques concernent plutôt les algorithmes de chiffrement par blocs comme le DES et l'AES,

- l'analyse de l'information mutuelle (MIA) dans laquelle c'est l'information mutuelle entre la modélisation de la fuite liée à la donnée sensible d'une part et la consommation de courant observée d'autre part qui fournira un test d'hypothèse sur la clé, y compris dans le cadre d'un modèle de consommation de courant non linéaire.

Dans les analyses de consommation de courant du type DPA/CPA, il est nécessaire de pouvoir calculer une valeur intermédiaire du calcul cryptographique sous une hypothèse de clé donnée. Cette prédiction de valeur intermédiaire n'est possible qu'à la condition de connaître la valeur de l'entrée (ou de la sortie) de la fonction cryptographique, et uniquement si l'implémentation n'est pas protégée par une contre-mesure de type masquage aléatoire des données.

** Thème d'étude principal

Dans le cas où ni le clair, ni le chiffré ne sont connus de l'attaquant, ou bien si un masquage aléatoire est implémenté, la valeur intermédiaire que doit prédire l'attaquant n'est plus disponible et l'attaque ne peut donc pas être menée sous sa forme classique.
Néanmoins, même si les valeurs elle-mêmes sont inaccessibles pour chaque exécution individuelle, les distributions de ces valeurs, et plus généralement les distributions jointes de plusieurs valeurs intermédiaires sont mesurables et peuvent être confrontées à leurs

distributions théoriques. Si les valeurs intermédiaires cibles sont choisies judicieusement, alors leur distribution jointe théorique peut être fonction de la valeur d'une partie de la clé (sous-clé), et nous pouvons donc nous baser sur celle-ci pour définir un distingueur (test d'hypothèse) des différentes valeurs de la sous-clé.
L'objet principal de cette thèse est donc d'étudier ce que pourrait être l'apport de nouvelles techniques d'analyses de canaux auxiliaires qui seraient basées sur l'étude de la distribution expérimentale de la fuite, et la comparaison de cette distribution avec un ensemble de distributions théoriques présumées.

** Thème d'étude secondaire

Même si les conditions requises pour pouvoir prédire les valeurs intermédiaires sont réunies (connaissance du clair ou du chiffré, et non randomisation des données), l'attaque différentielle (DPA) ou par corrélation linéaire (CPA) ne pourra fonctionner que si les traces de courant sont alignées, c'est à dire que, sur l'ensemble des traces, à chaque instant correspond toujours la même instruction/opération dans le déroulement du calcul.
Vis-à-vis de cette condition nécessaire supplémentaire, il est également intéressant d'étudier comment un attaquant pourrait passer outre une randomisation temporelle des traces, qui est une contre-mesure fréquemment implémentée.
Un autre volet de cette thèse pourrait donc s'atteler à étudier comment une analyse statistique de l'information globale (et non plus à chaque instant, pris individuellement) contenue dans les différentes traces pourrait permette de corréler la fuite présente dans cet ensemble de consommations avec la valeur de la sous-clé.

Compétences à l'issue de la thèse :

Un très bonne connaissance du domaine des analyses de canaux auxiliaires.
Un bonne connaissance de la cryptologie en général, et celle utilisée dans les cartes à puce en particulier.
Éventuellement, une bonne connaissance des attaques par analyse de fautes.
La capacité de poursuivre, en équipe autant que de manière autonome, la recherche dans le domaine des attaques physiques sur cartes à puce.

Présentation de l'équipe d'accueil :

L'équipe Cryptis est l'équipe de recherche adossée au master Cryptis de l'université de Limoges. Parmi les thématiques de recherches de cette équipe se trouvent la cryptologie et la sécurité des implémentations qui sont les composantes principales de ce sujet de thèse.

Financement : Lot 2: Sujet avec demande de financement institutionnel en cours

Spécialité de Doctorat : Sciences et Technologies de l'Information et de la Communication

Domaine de compétences principal: Informatique-Electronique

Domaine de compétences secondaire: Mathématiques

Candidat :

Compétences souhaitées : Étudiant de niveau bac+5 ayant de bonnes connaissances de base en cryptographie, sécurité de l'information, et un très bon niveau de programmation en langage C. Des compétences en sécurité physique des cartes à puce et en statistiques sont recommandées.

Conditions restrictives de candidature : Aucune

Date Limite de candidature : 4 Juin 2016 - 18h