2023

Hélène Le Bouder, Ronan Lashermes et Fabien Autrel

Sécurité matérielle : les attaques physiques

Leçon 2 : *Premières attaques*

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Objectifs Pédagogiques :

- Connaître les différents niveaux d'abstraction.
- Comprendre la différence entre une attaque par observation et une attaque par injections de fautes.
- Combiner des attaques physiques et logiques.
- Coder en temps constant, notamment un "personal identification number (`PIN`) code".

Table des matières

1 Introduction

Dans la leçon précédente, les cibles des attaques physiques étaient présentées. Dans cette leçon, les principes généraux des attaques physiques sont présentés. Historiquement, les premières attaques physiques furent des attaques temporelles [1]. Aussi elles sont le sujet d'une partie de la leçon.

2 Différents niveaux d'abstraction

Un **système informatique** est un ensemble d'éléments de type logiciel (software) et matériel (hardware), mis ensemble pour collaborer dans l'exécution d'un algorithme.

Entre l'algorithme conçu de manière théorique et sa mise en pratique dans un circuit (appelée aussi implémentation logicielle ou matérielle) il y a différents niveaux d'abstraction. À chaque niveau d'abstraction, de nouvelles failles sont possibles, c'est pour cela que les algorithmes théoriques ne peuvent pas anticiper toutes les attaques (présentes et futures) à la fois. Nous donnons la liste exhaustive des différents niveaux.

1. **Algorithme :** la représentation abstraite.
2. **Logiciel :** langage de programmation : C, java, python, *etc.* Une fois conçu, l'algorithme est décrit par un informaticien en langage de programmation. Le programme est alors compilé afin d'être traduit en langage machine en un ensemble d'instructions.
3. **Architecture de la machine et micro-architecture :**
   le **processeur** ou CPU est le composant de l'ordinateur qui exécute les instructions machines. Un processeur construit en un seul circuit intégré est appelé **microprocesseur**. Un programmeur peut choisir de coder en assembleur (langage machine). Ce langage représente le langage machine sous une forme lisible par un humain.
4. **Circuits logiques :**
   une instruction de type ALU se décompose en fonctions booléennes. Elles sont mises en œuvre en électronique sous forme de portes logiques. Une porte logique réalise des opérations booléennes sur une séquence de bits.
5. **Transistors :** dispositifs semi-conducteurs qui permettent de contrôler un courant (ou une tension). Les portes logiques sont construites à partir de plusieurs transistors connectés de manière adéquate. Dans un transistor, un 0 logique correspond à une tension en dessous d'une certaine valeur sinon cela correspond à un 1 logique.

Les attaques physiques se situent aux niveaux circuit logique et transistors.

3 Attaques par observation

Les **attaques par observation** appelées aussi parfois attaques par canaux auxiliaires [1] notées SCA se base sur l'observation du circuit pendant l'exécution des calculs.

Si un algorithme est théoriquement "sûr", le circuit dans lequel il est implémenté ne l'est pas forcément. C'est la frontière entre la théorie et la pratique. L'algorithme est théorique, le circuit lui est bien concret. Ainsi ce dernier a une consommation de courant, un temps de calcul, etc. Ce sont ces paramètres physiques qui peuvent nuire à la sécurité de notre algorithme. Ces paramètres ne sont pas faciles à anticiper d'un point de vue théorique, on parle de **fuite physique d'information** par un canal auxiliaire.

Ce type d'attaque est théoriquement non-invasive ; en pratique, l'attaquant peut vouloir acquérir des mesures à un emplacement précis du circuit et finalement la réalisation implique une attaque semi-invasive voir invasive.

Attention, il ne faut pas confondre les attaques par canaux auxiliaires avec les attaques par canaux cachés. Les attaques par canaux cachés exfiltrent de l'information via un canal caché. Ce n'est pas le sujet de ce cours.

1. Attention la définition de ce terme peut varier dune communauté scientifique à une autre.

4 Attaques par injections de fautes

Les **attaques par injections de fautes** notées FIA exploitent l'effet d'une perturbation intentionnelle sur le fonctionnement du circuit.

Les attaques par injections de fautes se basent sur l'idée de venir perturber le circuit. Pour une attaque, une ou plusieurs injections peuvent avoir lieu. Chaque injection conduit à une perturbation appelée faute. Deux cas se distinguent alors, le comportement normal du circuit et le comportement perturbé.
Les attaques FIA sont généralement puissantes. Cependant, elles ont le risque non négligeable d'**endommager** voir de **détruire** le circuit.

5 Exemple : les attaques temporelles

5.1 Définition

Le concept d'attaque temporelle a été introduit par Kocher [2] en 1996. Il consiste à mesurer le temps d'exécution d'un algorithme afin d'en déduire de l'information. Par exemple, lors d'un branchement conditionnel, deux branches différentes de code peuvent être appelées :

- une branche de code qui correspond au cas où la condition est vérifiée ;
- une branche de code qui correspond au cas où la condition n'est pas vérifiée.

Ces deux branches de code peuvent néanmoins présenter des différences de temps d'exécution. L'exploitation de cette différence pour obtenir de l'information est un exemple d'attaque temporelle.

Dans un algorithme si un biais temporel permet de retrouver une information sensible, alors l'algorithme doit être codé en temps constant.

5.2 Attaque temporelle contre le code `PIN`

Historiquement une des premières attaques physiques réalisées, est une attaque temporelle contre le code `PIN` des cartes à puces. En effet, à cette époque les algorithmes de vérification de codes `PIN` n'étaient pas en temps constant. À priori si le code `PIN` d'une carte à puce vaut 3141 et que l'utilisateur propose 0000 comme `PIN` candidat, dés le premier chiffre un algorithme de vérification de code `PIN` peut retourner `Faux`. Si c'est le cas, un attaquant peut mesurer le temps de réponse et attaquer chiffre à chiffre le code `PIN`.
Il y a donc nécessité de limiter le nombre d'essais.
Une telle attaque temporelle contre le code `PIN` peut se combiner avec une attaque par arrachage. Une **attaque par arrachage** est un terme historique qui désigne l'arrachage d'une carte à puce de son lecteur. Ainsi l'attaquant peut décider l'arrachage si le programme de vérification de code `PIN` entre dans le branchement qui traite un `PIN` candidat invalide. Il espère ainsi ne pas décrémenter le compteur d'essai.

En conclusion, si la vérification de code `PIN` n'est pas en temps constant, la combinaison évaluation du temps de calcul avec un arrachage de carte permet de retrouver le code `PIN` très rapidement.

6 Conclusion

Dans cette leçon, les différents niveaux d'abstraction ont été présentés. Aussi les attaques physiques se déroulent aux niveaux les plus bas (transistors et circuits logiques) pour attaquer le niveau le plus haut (l'algorithme théorique). Les attaques physiques se classifient en 2 familles à savoir les attaques par observation et les attaques par injections de fautes. Dans la famille des attaques par observation les attaques temporelles exploitent le temps de calcul d'un circuit. Dans les leçons à venir, nous verrons d'autres paramètres physiques exploitables.

Acronymes

PIN personal identification number. 2, 4

ALU arithmetic logic unit. 3

CPU central processing unit. 3

FIA fault injection attack. 4

SCA side channel analysis. 3

Références

[1] Jean-Francois Dhem, Francois Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, and Jean-Louis Willems. A practical implementation of the timing attack. In *International Conference on Smart Card Research and Advanced Applications*, pages 167–182. Springer, 1998.

[2] Paul Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. In *Advances in Cryptology - Crypto'96*, pages 104–113, New-York, 1996. Springer-Verlag.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

IMT Atlantique Bretagne - Pays de la Loire - www.imt-atlantique.fr

Campus de Brest
Technopôle Brest-Iroise
CS 83818
29238 Brest Cedex 03
T +33 (0)2 29 00 11 11
F +33 (0)2 29 00 10 00

Campus de Nantes
4, rue Alfred Kastler - La Chantrerie
CS 20722
44307 Nantes Cedex 03
T +33 (0)2 51 85 81 00
F +33 (0)2 51 85 81 99

Campus de Rennes
2, rue de la Châtaigneraie
CS 17607
35576 Cesson Sévigné Cedex
T +33 (0)2 99 12 70 00
F +33 (0)2 99 12 70 08