2023

Hélène Le Bouder, Ronan Lashermes et Fabien Autrel

Sécurité matérielle : les attaques physiques

Leçon 1 : *Les cibles*

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

Objectifs Pédagogiques :

- Prendre conscience de l'existence physique des circuits.
- Différencier une attaque logique d'une attaque physique.
- Prendre connaissance des contraintes liées à l'embarqué.
- Comprendre les notions d'authentification et d'usurpation d'identité.
- Découvrir le concept de code `PIN`.
- Comprendre le concept d'attaque par force brute.

Table des matières

1 Introduction

[1] Commençons par une simple énigme. Une pièce contient une ampoule éteinte, vous êtes à l'extérieur de cette pièce avec trois interrupteurs sur position "off ". Vous pouvez manipuler comme vous le souhaitez les interrupteurs, mais vous ne pouvez entrer qu'une seule fois dans la pièce. Comment déterminer quel interrupteur allume l'ampoule ?

La solution de cette énigme est la suivante. Allumez un premier interrupteur et attendez quelques minutes avant de l'éteindre. Ensuite, actionnez un deuxième interrupteur et entrez dans la pièce. Si l'ampoule est allumée, c'est le deuxième interrupteur que vous venez juste d'actionner qui dirige. Sinon, l'ampoule est éteinte. Touchez-la. Si l'ampoule a été allumée, elle est encore chaude. Dans ce cas l'interrupteur la commandant est le premier que vous avez manipulé. Si l'ampoule est froide, elle n'a jamais été allumée, il s'agit du dernier interrupteur que vous n'avez pas touché.

Si vous n'avez pas trouvé la solution à cette énigme, c'est que vous n'avez pas pensé à prendre la température de l'ampoule en considération. Vous avez raisonné de manière logique sur les possibilités on/off des interrupteurs et donc de manière uniquement théorique.

Quand on parle de sécurité informatique, la plupart des gens pensent aux mathématiques et à la cryptographie au sens logique théorique, mais peu pensent à la physique. Or, nos téléphones portables, nos cartes bancaires, nos ordinateurs, nos tablettes... sont constitués de circuits électroniques qui sont réels et non des outils théoriques. Aussi respectent-ils les lois de la physique liées au temps, à l'électricité, à la température, etc. C'est dans la physique que se cachent actuellement de nombreuses failles de sécurité, extrêmement difficiles à anticiper.

Introduction reprise de [1].

L'objectif de ce cours est la sensibilisation aux attaques physiques. Ces attaques sont trop souvent méconnues, bien que leur menace soit réelle. Cette première leçon est dédiée à la compréhension du concept des attaques physiques et surtout aux cibles de ces attaques.

2 Attaques physiques

Un algorithme de sécurité (cryptographique par exemple) est conçu pour être mathématiquement robuste. Cependant, une fois implémenté dans un circuit, un attaquant qui a physiquement accès au circuit peut utiliser les failles de ce dernier. Les **attaques physiques** sont l'ensemble des techniques d'attaques exploitant le fonctionnement du circuit. Ces attaques nécessitent donc un accès physique au circuit.

Il existe deux grandes familles d'attaques physiques :

- les **attaques par observation** ;
- les **attaques par injection de faute**.

Ces deux familles d'attaques sont présentées en plus ample détails dans les leçons suivante.

3 Les cibles des attaques physiques

3.1 Les système embarqués

On observe depuis quelques années, une augmentation de l'utilisation de petits circuits connectés ou non dans la vie quotidienne.

Un **système embarqué** est un système informatique avec trois caractéristiques particulières :

1. une fonction spécialisée,
2. des contraintes d'encombrement,
3. des contraintes énergétiques.

1. illustration : Pixabay

L'exemple le plus répandu de système embarqué est la **carte à puce** car elle est utilisée notamment pour les transactions bancaires [2, 3]. Plusieurs brevets ont été déposés dans les années 70-80. Contrairement à ce que beaucoup prétendent, la carte à puce n'est pas une invention exclusivement française. Aussi, plusieurs ingénieurs peuvent se revendiquer être les inventeurs de la carte à puce, à savoir : le japonnais Kunitaka Arimura, le français Roland Moreno [4] et les allemands Helmut Gröttrup et Jürgen Dethloff.

3.2 Cas d'usages des attaques physiques

Les attaques physiques permettent d'obtenir des informations sur un circuit. Elles sont utilisées pour les deux principaux différents usages suivants.

1. La **recherche** d'un secret comme un secret cryptographique ou un code `PIN` a généralement pour but :
   - de voler des données personnelles, contenues dans le circuit attaqué.
   - ou d'obtenir des droits, pour avoir accès à de nouvelles fonctions (exemple des consoles de jeux) ou pour se connecter à un réseau.
2. La **rétro-conception** est l'activité qui consiste à étudier un objet pour en déterminer le fonctionnement interne. Elle est souvent utilisée à des fins d'espionnage industriel.

Il est important de faire remarquer que les attaques physiques contre l"internet of things (IoT)" peuvent se cumuler avec des attaques sur le réseau. En effet, après avoir pris le contrôle d'un objet connecté, cet objet peut nuire de multiple façon, comme l'envoie d'information falsifiée, le ralentissement du réseau, voir si plusieurs objets sont corrompus lancer une attaque par déni de service.

4 Cas usage proposé dans le MOOC

4.1 Authentification

Une **authentification** permet de valider l'origine d'une entité.

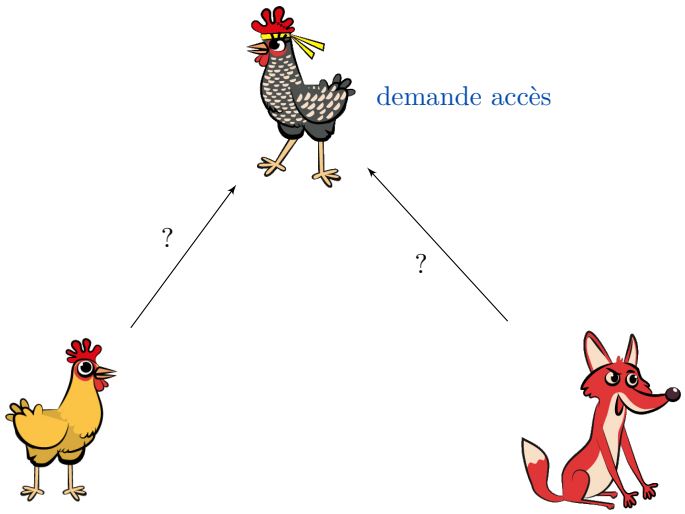

FIGURE 1 – Authentification

Pour cela en cryptographie on peut utiliser une signature numérique, mais ce n'est pas l'unique moyen. Pour authentifier quelqu'un, on peut aussi obtenir une combinaison des éléments suivants.

- que l'on possède,
- que l'on connaît,
- que l'on est.

L'**usurpation d'identité** est le fait de prendre délibérément l'identité d'une autre entité (personne ou machine), dans le but d'avoir accès à des données ou droits. L'authentification a pour but de contrer une usurpation d'identité.

4.2 PIN code

Un code de type **personal identification number (PIN)** est un code confidentiel, destiné à authentifier le titulaire d'une carte à puce. Dans ce cas, nous avons un couple (identifiant, mot de passe). La carte est l'identifiant que le titulaire possède. Le code PIN est le mot de passe que seul le titulaire de la carte connaît.

Parce qu'il est utilisé dans un contexte bancaire, le code PIN est la cible de nombreuses attaques.

L'attaque la plus triviale est l'attaque par force brute. Une **attaque par force brute** consiste à tester, une à une toutes les combinaisons possibles d'un secret (code, mot de passe, clé, etc.) jusqu'à trouver sur la valeur exacte. Il est important de rendre ce type d'attaque impossible soit en limitant le nombre d'essais à l'attaquant soit en ayant un nombre de possibilités sur le secret trop grand. Actuellement on considère que 2^{80} est le nombre minimum inatteignable.

5 Conclusion

Dans cette première leçon, l'intuition des attaques physiques a été amenée. Il ne faut pas baser la sécurité d'un circuit uniquement sur la logique, mais prendre en compte la dimension physique de celui-ci. Dans les leçons suivantes, les différentes familles sont présentées.

Le cas d'usage pour illustrer les attaques physiques dans les futures leçons a été introduit. Il s'agit d'une authentification par code PIN pour un système embarqué type carte à puce.

Acronymes

PIN personal identification number. 2, 4, 5

IoT internet of things. 4

MOOC massive open online course. 2, 4

Références

[1] Hélène Le Bouder. Des attaques informatiques utilisant la physique. *Interstices*, 2016.

[2] Musée art et Métiers. Carte à puce. une histoire à rebonds. https://www.arts-et-metiers.net/musee/carte-puce-une-histoire-rebonds.

[3] Arnaud Tisserand. Piratage de cartes à puces : comprendre comment ça marche. http://www.slate.fr/story/152207/piratage-cartes-puces-comprendre-comment-marche.

[4] (roland moreno, un woody allen de la technique.

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