Université de Boumerdès

Faculté des Sciences de l'Ingénieur

Spécialité: Electronique des systèmes embarqués

Module: Cartes à puces

Chapitre 3: Cryptographie

Dr. Messaoudi Belkacem Samia

2021/2022

Plan

1. Généralités

1)Introduction

- La cryptographie est l'art de chiffrer et déchiffrer les messages échangés entre un émetteur et un récepteur
- Il existe deux schémas classiques de chiffrement
  - Symétrique qui utilise la même clé pour le chiffrement et le déchiffrement
  - Asymétrique avec une clé publique et une clé privée générées par une procédure mathématique comme dans l'algorithme RSA
- Seules les cartes dotées d'un crypto processeurs permettent de gérer le chiffrement asymétrique

1)Introduction

- Cryptosysteme
- Cryptanalyse

2) Sécurité

L'ISO 78 a défini 6 services de sécurité :

- authentification (de la source et/ou du destinataire) ; contrôle d'accès (qui nécessite une authentification préliminaire) ;
- confidentialité des données (les données illicitement récupérées doivent être inutilisables);
- intégrité des données (empêcher les modifications des données, les doublons) ;
- non-répudiation (un message, son envoi et sa réception ne peuvent être contestés) ;
- protection de l'analyse du trafic (la relation entre deux personnes doit rester secrète).

2)Sécurité

- Objectifs du fraudeur
  - Obtenir l'accès à une information
  - Corrompre des informations
  - Réfuter l'envoi ou la réception d'une information
  - Provoquer la méfiance vis à vis d'un système
- Attaques :
  - Se faire passer pour quelqu'un d'autre
  - Empêcher le fonctionnement correct d'un système
  - Corrompre un protocole pour obtenir des secrets
  - S'insérer dans le système comme relais actif

2)Attaques

- Physiques
- Logiciels

2.1) Attaques physiques

- Deux critères principaux
- Comportement de l'attaquant
  - Actif: il agit, modifie le comportement du circuit
  - Passif: il observe certains propriétés physiques du circuit
- Degré d'implication de l'attaquant
  - *Invasive: il n'a aucune limite (coûteux)*
  - *Semi-invasive: il peut enlever le packaging mais ne touche pas à la structure interne du circuit (abordable)*
  - *Non-invasive: observe et manipule le circuit sans modifications physiques (très peu coûteux)*

Chiffrement césar

Il s'agit d'un des plus simples et des chiffres classiques les plus populaires. Son principe est un décalage des lettres de l'alphabet (**substitution mono-alphabétique**)

Pour le chiffrement, on aura la formule

$$C = E(p) = (p + k) \bmod 26$$

CLAIR	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
-> décalage = 3																										
CODE	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

exemple : d'après cette méthode, "VIVE LES MATHS" devient donc "YLYH OHV PDWKV" !

Chiffrement césar

Sécurité :

- Il n'existe que 26 décalages possibles (**attaques exhaustives**),
- Le chiffre de César est très vulnérable à **l'analyse des fréquences**

Implémentation (matlab)

Chiffrement césar :

```
clear all;clc;close all
text=input('entrer un text :','s');
db=double(text);
N=input('entrer le nombre de decalage :');
type=input(':');
h=((text+N)-97);
cesar=mod(h,26);
f=(cesar+97);
crypt=char(f);
disp('votre text crypté est : ')
disp(crypt)
```

Déchiffrement césar :

```
h=((text-N)-97);
cesar=mod(h,26);
f=(cesar+97);
message=char(f);
disp('votre text decrypté est : ')
disp(message)
```

Attaques physiques principales

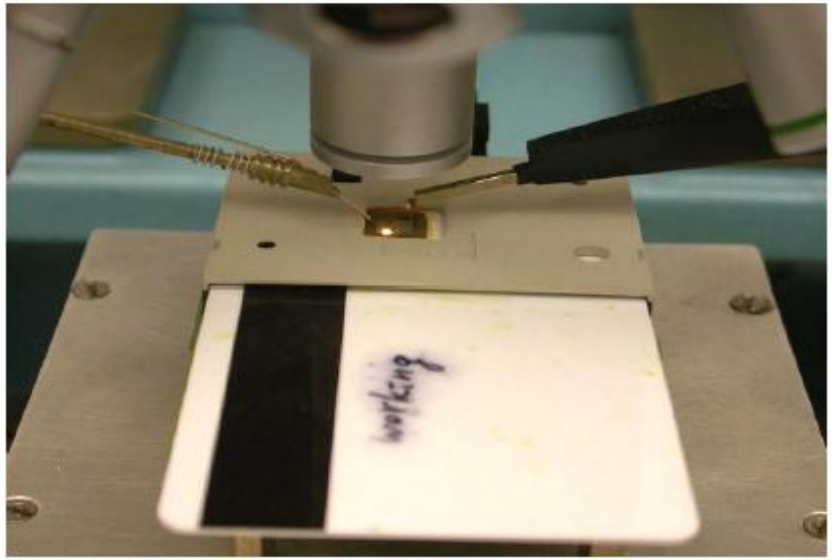
	Active	Passive
Non-invasive	Glitching, changement de température, faible voltage, …	Attaques par canaux cachés (*side-channel attack*)
Semi-invasive	Attaques par lumière, radiation, …	Attaques EM, inspection optique
Invasive	FIB	Probing

Attaque active invasive

- Le composant est manipulé et modifié par l'attaquant
- Le circuit peut être modifié par un *focused ion beam (FIB) (sonde ionique focalisée)*
- Equipement **très coûteux mais possibilités énormes pour l'attaquant**

Attaque active semi-invasive

- Injection de faute (*fault attack)*
  - Composant dépackagé et placé sous un microscope
  - Les transistors peuvent être changés d'état par une lumière forte et focalisées (laser)



Attaque active non-invasive

- Perturber le fonctionnement du composant sans le dépackager
- *Glitching*
  - Perturber l'alimentation en courant du composant pendant son fonctionnement peut provoquer des sauts d'instruction
  - Perturber l'horloge extérieure peut provoquer des corruptions de données ou des sauts d'instruction
- Température
  - Modifications aléatoires dans la RAM
  - Opérations de lecture erronées dans les NVMs

Attaque passive invasive

- *Microprobing:*
  - Sonder des signaux sur le composant à l'aide de microprobes
  - Injection de signaux et observation des réactions du composant
  - Sert à extraire des clés secrètes ou du contenu de mémoire

Attaques passive semi-invasive

- Attaques *side-channel qui demande de dépackager le composant: émanations EM*
- –Plus coûteux
- –Plus précis que la consommation de courant

attaque passive non-invavise : side-channel attacks

- Idée: révéler le secret en observant les propriétés physiques du composant
- *Timing attack*
  - Mesure le temps d'exécution
- *Power attack*
  - Mesure la consommation de courant
  - Peu coûteux en équipement: un PC avec un oscilloscope et une petite résistance sur l'alimentation en courant du composant
  - Attaque très efficace
  - Deux méthode basiques: attaque simple (SPA) et différentielle (DPA)

SPA (Single Power Analysis)

- SPA utilise les motifs présents dans l'implémentation qui sont liés aux données sensibles
- Stratégie d'attaque
  - Connaître l'algorithme utilisé
  - Phase de reverse engineering

Contremesure SPA

- Pas de code conditionnel sur des données secrètes
- Contremesure au niveau algorithme
  - Structure du code
  - Randomisation des données
- Contremesure au niveau hardware
  - Ajouter du bruit
  - Désynchronisations

Differential Power Analysis

- La DPA est un moyen d'isoler et d'augmenter l'effet des faibles contributions des bits des données sur un large ensemble de courbes de consommation
- Il est souvent difficile de repérer la différence de consommation entre le traitement de 2 données

DPA (Differential Power Analysis)

- La DPA utilise un nombre important de courbes de consommations
- La fonction crypto attaquée est exécutée avec des entrée connues et différentes
- L'attaquant choisit un bit intermédiaire d'une valeur qui dépend du secret (et des entrées)
- Quand ce bit est traité, la courbe de consommation va légèrement dépendre de sa valeur
- En séparant les courbes en 2 ensembles suivant le bit, la différence de leur moyenne montre une différence si (et quand) le bit est traité

Comment se protéger de ces attaques?

- Estimer le danger: comprendre les enjeux, le coût, la probabilité
- Développer des protections adéquates aux point faibles
- Faire une évaluation de sécurité
- Choisir des composants sûrs pour construire le système à cryptographie forte

Conclusions

- Il n'existe pas de protection absolue
  - Avec assez de temps et ressources toute contremesure peut être cassée
- L'objectif en pratique est de rendre un système tellement cher à attaquer que ce n'est plus rentable pour un attaquant
- Domaine en constante évolution
  - Protections doivent tenir compte des possibles évolutions du matériel et techniques des attaquants