M2 Cybersecurity - Smart Card Security

Charles Guillemet
Janvier 2017 – 50 mn
January 2017 – 50mn

Les documents papiers ne sont pas autorisés. *Paper documents are not permitted.*

1ere partie/1rst Part : Smart Card Security

1- Répondre aux questions de manière concise (~3 lignes par question) [Barème : 5/20]
Answer briefly the following questions (~3 lines for each question) [Rate : 5/20]

Qu'est-ce que la rétro-conception ?
What is reverse engineering?

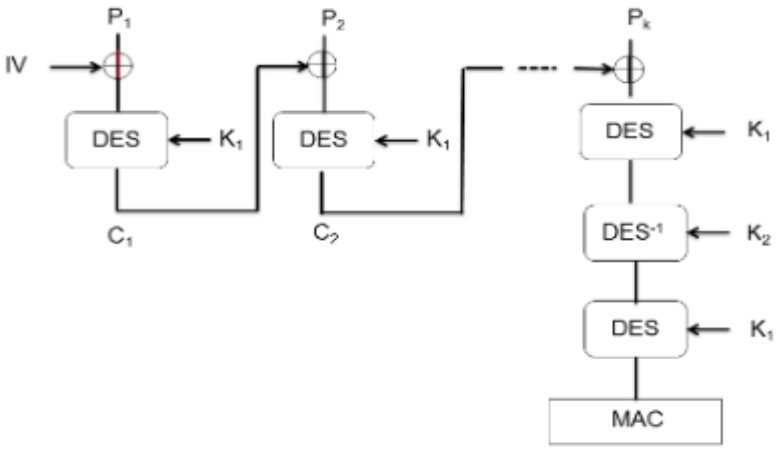
Qu'est-ce que le « RSA-CRT » ? Pourquoi est-il utilisé ? Est-il plus sécurisé que le RSA direct ?
What is RSA-CRT? Why is it used ? Is it more secure than straightforward RSA?

Décrivez ce que sont les attaques par canaux auxiliaires sur carte à puce, et tout particulièrement l'attaque DPA. Quel est le principe de la DPA ? Quelles sont les hypothèses d'application ?
Describe what is Side Channel Analysis, and specially Differential Power Analysis. How DPA works? What are the requirements to apply these attacks?

2- **Attaque sur le Retail MAC. [Barème : 8/20].**
Attack on Retail MAC. [Rate: 8/20].

Dans tout cet exercice, on suppose qu'un attaquant peut faire appel à des hackers proposant le service suivant :
Connaissant l'entrée E et la sortie S d'un simple DES, les hackers peuvent retrouver par force brute (et grâce à une puissance de calcul qu'ils ont) les 56 bits de clef DES K (où S = DES(E, K)).
In the whole exercise, we consider that an attacker can call hackers who propose the following service:
Knowing the input E and the output S of a simple DES, hackers can retrieve by brute force (and thanks to powerful computation systems they dispose) the 56 bits of the DES key (where S = DES(E, K)).

On considère l'algorithme suivant appelé Retail MAC:
We consider the following algorithm named "Retail MAC":



Où P est le message d'entrée composé de k blocs de 64 bits chacun P1 || P2 || … || Pk et IV = 0.
Where P is the input message composed of k 64-bit blocks P1 || P2 || ... || Pk and IV = 0.

a) A partir du schéma ci-dessus, identifier les éléments connus des éléments non connus parmi: IV, P1, K1, C1, P2, C2, Pk, K2, et MAC.
From the above chart, identify the known elements from the unknown ones among: IV, P1, K1, C1, P2, C2, Pk, K2, and MAC.

L'attaquant dispose d'un oscilloscope et veut attaquer l'algorithme de MAC grâce à une analyse en observation (canaux auxiliaires).
The attacker has access to an oscilloscope and wants to attack the MAC algorithm thanks to an observation analysis (side channel).

i) l'attaquant veut récupérer la clef K1 du premier DES du MAC, pourquoi ne peut-il pas y arriver directement grâce à une force brute ?
i) the attacker wants to retrieve the K1 key of the first DES of the MAC, why is the attacker not able to retrieve it thanks to a brute force?

ii) on suppose maintenant qu'il cherche à faire une attaque afin de retrouver C1, il se focalise alors sur l'opération XOR avec P2. Puisqu'il connaît P2 mais pas C1, quelle attaque en observation peut-il faire sur cette opération ?
Expliciter succinctement le protocole opératoire.
ii) we now suppose that the attacker wants to conduct an attack in order to find C1, the attacker focuses onto the XOR operation with P2. As P2 is known but not C1, what observation attack can be done onto this operation?
Briefly explain the operating protocol.

iii) On suppose que l'attaquant est capable de retrouver C1. Peut-on retrouver K1 ? K2 ?
It's supposed that the attacker is able to retrieve C1. Is it possible to retrieve K1? K2?

3- Attaque en faute sur multiplication scalaire ECC [Barème : 7/20]
Fault attack on a scalar multiplication (ECC) [Rate: 7/20]

On dispose d'une carte à puce qui exécute des multiplications scalaires sur une courbe elliptique donnée.
Etant donnés un scalaire d (inconnu) et P un point public, elle calcule dP, et renvoie cette valeur en sortie.
Un attaquant dispose d'un laser permettant d'injecter une faute sur un des bits de d. Chaque tir change un des bits de d. Chaque bit peut être fauté avec une probabilité similaire.
Let a smartcard used to compute scalar multiplications on a given elliptic curve. Given a scalar d (unknown) and a public point P, it computes dP and sends this value as output.
An attacker has access to a laser which allows to inject a fault on a single bit of d. Each laser shot switches one of the bits of d. Each bit can be faulted with the same probability.

1. Comment exploiter cette vulnérabilité afin de retrouver le scalaire privé d ?
   How to exploit this vulnerability in order to retrieve the private scalar d?
2. Proposer des contremesures pour parer cette attaque.
   Propose countermeasures to counter this attack.