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?

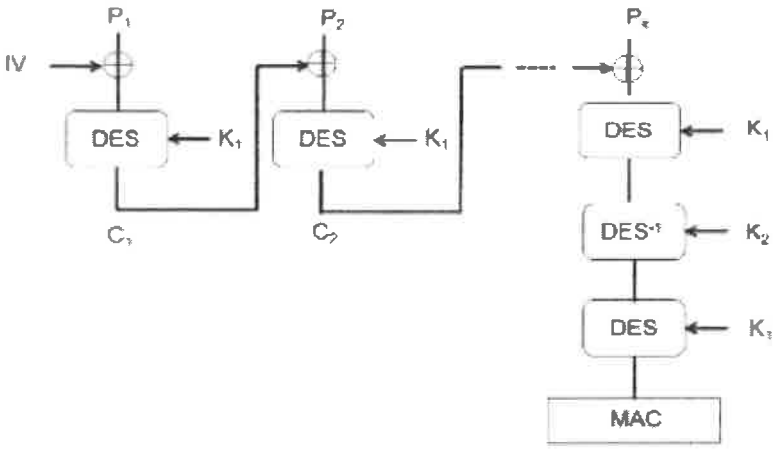
Qu'est-ce que le « RSA-CRT » ? Pourquoi est-il utilisé ? Est-il plus sécurisé que le RSA direct ?
What is RSA-CRT? Why is it used ? Is it more secure than straightforward RSA?

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.

ANIOT Simon Valentin 15/20
SAHAR Boris 14,5
BOUGUERA Amine 13,5
BOULAY Ludovic 15
BRUNETTI Rodolphe 15
FURFARO Francisco 12
MADELON Alexia 19
MIAVRIL Valentin 13
MONNET-PAQUET Aurélien 10
PEYNET Benoit 13,5
PUTEAUX Pauline 16
RIBAUCOURT Alice 14
SECKINGER Pascal 19,5
SELLAMI Louis 8,5
TRAN Dinh Cuong 11,5
TROUSSIEUX Samuel 11
VASSEUR Valentin 17
RAKOTOMANGA Mary Andrea 15,5

M2P SCCI / M2R SCCI - Smart Card Security

Charles Guillemet – Florent Autréau
14 janvier 2016 – Durée : 1h30

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

1ere partie/1rst Part : Smart Card Security

1- Répondre aux questions en détaillant comme vous le souhaitez. [Barème : 5/20]
Answer the following questions, giving as many details as you want. [Rate : 5/20]

Qu'est-ce que la rétro-conception ?
What is reverse engineering ? Is this a threat for circuits?

Un développeur de code de carte à puce doit il prendre des précautions particulières pour écrire un « bon » code ? Si oui, lesquelles ?
Does a smart-card software developer need to take special care to write a secure code?

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 ? Quel est le rapport entre la DPA et la corrélation ? Comment appliquer la DPA à l'algorithme AES ?
Describe what is Side Channel Analysis, and specially Differential Power Analysis. How DPA works? What is the link between DPA and correlation? How to apply DPA to AES?

2- Side Channel sur ECDH [Barème : 9/20]
Side Channel on ECDH. [Rate : 9/20]

Un développeur conçoit un système de contrôle d'accès. Les utilisateurs ont un badge sans contact. Afin d'entrer dans la zone protégée, un utilisateur doit présenter son badge ainsi que son doigt au lecteur.
Le lecteur extrait les minuties et digitalise l'empreinte digitale noté F.
Ensuite, un échange de clé basé sur ECDH est mis en place.
Le badge a une paire de clé $(d_T, Q_T = d_T G)$. Le badge a aussi l'empreinte de l'utilisateur dans sa mémoire. A chaque nouvelle utilisation, le lecteur génère une nouvelle paire de clés $(d_R, Q_R = d_R G)$.
Le protocole d'accès est le suivant :

1. Le badge envoie sa clé publique Q_T au lecteur qui l'identifie.
2. Le lecteur envoie Q_R au badge.
3. Le badge calcule $d_T Q_R$ et extrait les 128 bits de poids faible qui vont servir de clé AES notée K.
4. Le lecteur envoie $C = AES_K(F)$ au badge.
5. Le badge déchiffre C et le compare à l'empreinte enregistrée sur la carte (Match on Card). Si l'empreinte présentée correspond à l'empreinte enregistrée dans la carte, elle renvoie AUTH_OK au lecteur, sinon elle renvoie AUTH_FAILURE au lecteur.
6. Le lecteur ouvre l'accès ou non selon la réponse de la carte.

A developer designs a new access control system. The users have a contactless token. In order to enter in a protected zone, the user puts his token onto the reader and his finger on the fingerprint reader.

Then the reader extracts the minutiae and digitalizes the fingerprint (denoted F).
After that, an ECDH key agreement is applied.
The token has a pair of keys $(d_T, Q_T=d_TG)$ and also the user's fingerprint in its memory. Each time, the reader, generates a new pair of keys $(d_R, Q_R=d_RG)$. The access control protocol is the following:

1. *The token sends its public key Q_T to the reader which identifies the token*
2. *The reader sends Q_R to the token.*
3. *The token computes d_TQ_R and extracts the 128 Least Significant Bits. They will be used as AES key denoted K.*
4. *The reader sends $C=AES_K(F)$ to the token.*
5. *The token decrypts C and compares the fingerprint to the fingerprint written in the card (Match on Card). If the fingerprint matches the token sends AUTH_OK to the reader, otherwize it sends AUTH_FAILURE to the reader.*
6. *The reader grants the access or not regarding the token answer*

a) Quelle interface le badge utilise-t'il pour communiquer avec le lecteur ? *Which kind of interface does the token use to communicate with the reader?*
b) Comment le lecteur connait il la clé K ? *How does the reader know the key K?*
c) Y'a-t-il une faille dans ce protocole ? *Is there a weakness in the protocol?*
d) Si oui, modifiez ce protocole afin de le sécuriser. *If, yes modify the protocol in order to secure it.*

L'algorithme de multiplication scalaire est un algorithme appelé Double And Add. A partir du point P, et du scalaire d, il calcule dP. Voici le pseudo code de celui-ci.
The scalar multiplication algorithm implemented is called Double and Add. From the point P and the scalar d, it computes dP. Here is its pseudo-code.

Pour/for $d=[d_{m-1}, \ldots, d_0]$

```
Q ← 0
  for i from 0 to m-1 do
     if dᵢ = 1 then
         Q ← point_add(Q, P)
     P ← point_double(P)
  return Q
```

Pour P et Q, 2 points sur la courbe E d'équation $y^2 = x^3 + ax + b$/ *For P and Q, 2 points on the curve $E : y^2 = x^3 + ax + b$*

$$P + Q = R$$
$$(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$$

La fonction point_add est calculée de la façon suivante/ *The point_add function is computed as :*

$$x_r = \lambda^2 - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$
$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$

Et la fonction point_double est calculée de la même manière avec / *And the function point_double is computed the same way using:*

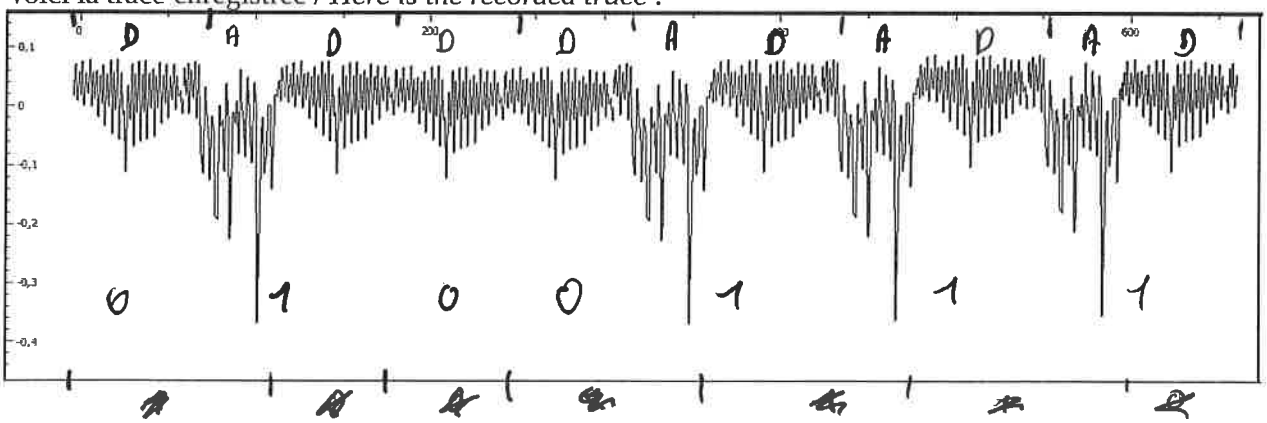
$$\lambda = \frac{3x_p^2 + a}{2y_p}$$

e) Montrer que cet algorithme calcule bien dP (on ne demande pas de prouver les formules point_double et point_add). / *Prove that the algorithm computes dP (proving point_double and point_add is not asked).*

f) Quelle est la complexité de cet algorithme ? *What is the computational complexity?*
- En nombre d'appels à point_add, point_double (meilleur cas, pire cas, cas moyen) ?
- *Number of point_add and point_double calls (worst case, best case, average case) ?*

g) L'algorithme est-il équilibré ? *Is this a balanced algorithm ?*

Un attaquant enregistre les émanations électromagnétiques du badge pendant l'échange de clé.
An attacker records the electromagnetic field of the token during the key exchange.
Voici la trace enregistrée / *Here is the recorded trace :*



h) Peut-on retrouver la clé privée du badge ? Que vaut-elle ? *Is it possible to retrieve the token secret key ? What is its value ?*

i) Proposez une contremesure. *Propose a countermeasure.*

j) Votre contremesure est-elle résistante à la Safe Error Attack ? Décrire la Safe Error Attack. Proposez une contremesure resistante contre la SPA et la safe error attack.
Is your countermeasure resistant against Safe Error Attack? Describe safe error attack. Propose a countermeasure resistant against SPA and safe error attack.

0111 0010

3- DFA RSA-CRT (seulement pour les étudiants M2P). [6/20]
DFA RSA-CRT (*only for M2P students*). *[Rate: 6/20]*

On dispose d'une carte à puce servant à signer des messages électroniques avec une clé privée RSA se situant à l'intérieur de la smartcard. La signature implémentée utilise le CRT. La formule implémentée est la formule de Garner.
En notant m, le message à signer, N le module public tel que N = p*q, e l'exposant public et d l'exposant privé, la carte calcule :
*Let a smartcard used to sign electronic message using a secret RSA key embedded inside the smartcard. The implemented signature uses the CRT. The implemented CRT uses Garner's formula. Denoting m the message to sign, N the public modulus such as N =p*q, e the public exponent, and d the private exponent, the smartcard computes:*

$$S = S_q + [(S_p - S_q) * q_{inv} \bmod p] * q$$

Un attaquant dispose d'un laser et est capable d'injecter une faute durant ce calcul. An attacker has a laser and is able to induce a fault during the computation.

k) Pourquoi utilise-t-on le CRT et pas l'exponentiation directe ? *Why the CRT is used (and not the straightforward exponentiation)?*
l) Démontrer qu'il est possible de casser le RSA. Expliquer comment. *Prove that, it's possible to break RSA. Explain How.*
m) Quelles sont les hypothèses de l'attaque ? *What are the hypothesis of this attack ?*
n) Que peut-on retrouver ? *What can you retrieve ?*

Un « petit » exemple / *a toy example :*
- N = 7181
- e = 5
- S = 4065 – la signature correcte / *the correct signature*
- S' = 5902 – une signature fautée / *a faulty signature*

o) Retrouver l'ensemble des paramètres qui peuvent l'être. *Find the parameters which can be.*
p) Proposer des contremesures. *Propose countermeasures.*

2eme partie/2nd Part : Java Card

Développement d'application JavaCard (seulement pour les étudiants M2R – à rendre sur une copie séparée). [Barème : 6 / 20]
JavaCard Application Development (only for M2R students – to be submitted on a separated sheet). [Rate : 6/20]

Étudier le codage suivant de la fonction `Verify Pin`. (Volontairement peu robuste par rapport à des attaques)
Study the implementation of the function Verify PIN (Poorly resilient against attacks)

```
1.  boolean verifyPIN (byte[] buffer, short ofs, byte len)
2.  {
3.   // No comparison if PIN is blocked
4.   if (triesLeft < 0)
5.    return false ;
6.   // Main comparison
7.   for(short i=0; i < len; i++)
8.    if (buffer[ofs+i] != pin[i])
9.    {
10.    triesLeft-- ;
11.    authenticated[0] = false ;
12.    return false ;
13.   }
14.  // Comparison is successful
15.  triesLeft = maxTries ;
16.  authenticated[0] = true ;
17.  return true ;
18. }
```

Cette méthode est elle fonctionnelle ? Décrire et commenter l'algorithme.
Does it work ? Describe and comment its algorithm.

Quelle attaque peut être menée par rapport à un arrachage comme pour les premières cartes à puce ? Quelle contre mesure suggèrez-vous ?
Evaluate its robustness against 'swipe-out' attack and suggest a counter-measure.

Et sur une attaque en temps? Quelle contre mesure serait efficace ?
Same question with a timing attack. What countermeasure do you suggest ?

Comment protéger `triesLeft` contre une attaque de type injection de faute ? Comment s'en prémunir ? Quelles sont les limites de la stratégie de protection ?
How to protect `triesLeft` against a fault injection attack ? Suggest a protection. What are the limitations of the proposed protection?

Trouver une contre mesure permettant de vérifier l'intégrité du flot complet d'exécution.
Suggest a countermeasure allowing to verify integrity of execution flow

maudlapsy@