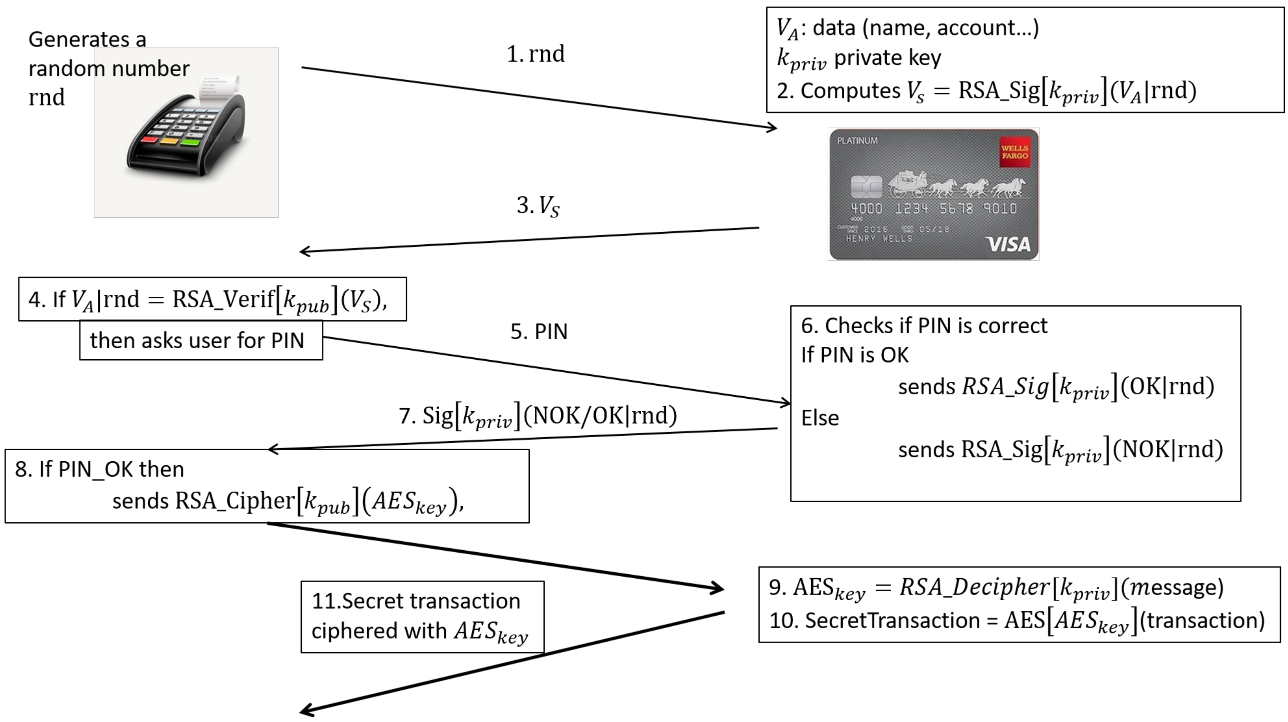
M2 Cyber Security - SmartCards Security - 2023
Breaking Banking cards

The goal of the test is to find the many vulnerabilities of a banking card protocol. Your target is the banking card and you have full control of the terminal, the communication channel. You have the knowledge of the RSA public key, k_{pub}. Each of the three following sections will be dedicated to retrieve secrets, k_{priv}, PIN and AES_{key} from the protocol described below.

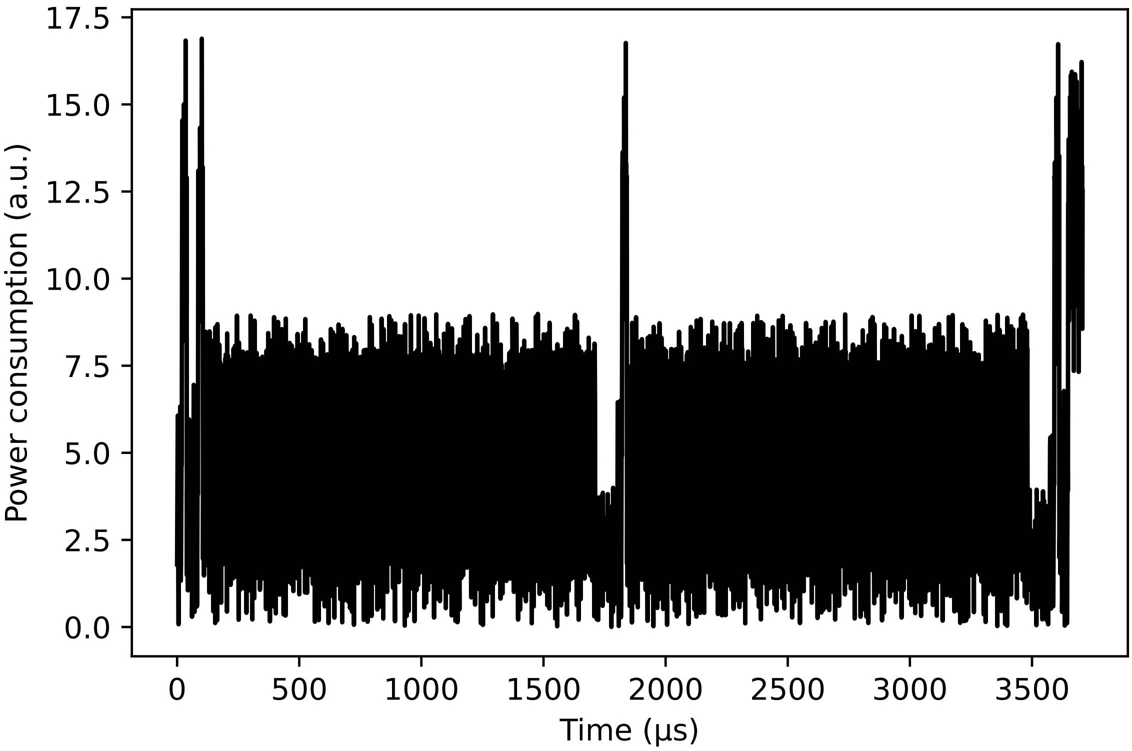


1. Attack on RSA - Steps 1–4 [11/20]

1.1. What is the purpose of Step 1 that sends a random number to the card? Which kind of attacks would you be able to perform if this number was always the same?

1.2. Is it possible and how would you make a random number more predicable?

The figure below shows a power trace of the SmartCard recorded during Step 2.



1.3. Describe the tools and the procedure needed to obtain such a signal.

1.4. Looking at the curves, the algorithm used here is obviously an RSA-CRT. Why?

1.5. Describe a Differential Fault Attack (DFA) on RSA-CRT. Given the specific protocol described above, could you succeed this attack?

Since RSA-CRT is too weak, the SmartCard developer modifies the RSA implementation, with the following classic algorithm, with d being the private key (which corresponds to k_{priv} in the protocol):

Algorithm 1 Calculate $C = M^d \mod n$ with $d = [d_{n-1}..d_0]$ d_0 being the Least Significant Bit. ex: d=0d13=0b1101 = [1101]

$C \leftarrow 1$, $R \leftarrow M$, $D \leftarrow M$
for $i = 0$ to $n-1$ **do**
  if $d_i = 1$ **then**
    $C \leftarrow C \times R \mod n$
    $R \leftarrow R^2 \mod n$
  else
    $R \leftarrow R^2 \mod n$
    $D \leftarrow C \times R \mod n$
  end if
end for
return C

1.6. Can you still fault this algorithm? Which means of perturbation would you use? How many faults would you need?

1.7. There is also a side-channel attack that will work on the algorithm. Find it and describe it briefly.

2. Verify PIN - Step 6 [5/20]

The PIN code verification at step 6 has been given by the developer. The goal of the attack is to authenticate yourself without knowing the real PIN code (i.e. function `Verify_PIN` shall return `true`). Number of tries is limited to 100 and controlled by variable `tries` stored in a Non Volatile Memory. When this variable is below 0, the function `kill_card()` destroys the SmartCard.

```
1 const int true = 0x1234;
2 const int false = 0x9876;
3 extern void kill_card(void);
4 int tries = 100; // permanently stored & updated in a Non Volatile Memory
5 int correct_PIN[4] = {9,8,7,6};
6
7 int verifyPIN_1(int user_PIN[]){
8   int correct_digits = 0;
9   if (tries < 0) kill_card();
10  tries--;
11  for (int i=0; i < 4; i++) {
12    if(user_PIN[i] != correct_PIN[i])
13      correct_digits --;
14    else
15      correct_digits ++;}
16  if (correct_digits == 4){
17    tries ++;
18    return true;}
19  else
20    return false;}
```

Explain the countermeasures at the following lines. Why and against which kind of attacks have they been inserted ?

2.1. lines 1-2

2.2. lines 12 to 15

2.3. lines 9 and 16

3. AES - Step 10 [4/20]

In this section, the attacker has NO more the control of the terminal, hence AES_{key} used in Step 8 is unknown. She can only observe the chip power consumption and listen to the communication channel.

3.1. Which kind of Side Channel Attack (SCA) can you perform: Differential Power Attack (DPA), Correlation Power Attack (CPA), Template Attacks? Why?

3.2. Which kind of protections against side channel attacks could you put in the chip? Describe at least one hardware and one software coutermeasures.