HWSec: exam

Renaud Pacalet

21 June 2017

You can use any document you need. Please number the different pages of your work and indicate on each page your first and last names. Write your answers in French or in English, as you wish, but avoid mixing the languages. If some extra information or hypotheses are missing to answer a question or solve a problem, decide by yourself and write down the added hypotheses or information. If you consider a question as absurd and thus decide not to answer, explain why. If you do not have time to answer a question or solve a problem but know how to, briefly explain your ideas.

Important advice #1: quickly go through the document and answer first the easy parts.

Important advice #2: copying verbatim the slides of the lectures or any other provided material is not considered a valid answer.

The first part is a set of five questions (2 points each) and the second part is a small problem (10 points).

1 Questions

1.1. Side channel attacks: in order to protect her DES implementation against side channel attacks, a security engineer decides to change the SBOxes of the standard and to replace them by carefully crafted ones and to keep them secret. What do you think of this?

1.2. Timing attacks against RSA: assuming you are in charge of protecting an RSA implementation against timing attacks, what countermeasure(s) would you implement and why?

1.3. Power attacks: the course enumerates different hypothesis for a power attack to be practical:

- H1: The attacker acquires a «large» number of traces with the same secret
- H2: The attacker knows the plain or cipher text of each trace
- H3: The attacker can make an hypothesis on the secret
- H4: The attacker can build a partition of the set of traces based on the hypothesis on the secret
- H5: The statistics of the subsets are significantly different when and only when the hypothesis is right
  - H5–1: The power is correlated with the processed data
  - H5–2: The SNR of the DPA signal is «good enough»

For each of them propose a countermeasure based on nullifying it and discuss the efficiency of such a solution.

1.4. Propose three different fault injection techniques and discuss their advantages and drawbacks on the attacker's point of view.

1.5. Blinding: why is it easier to implement blinding-based countermeasures for some cryptographic algorithms than for others?

2 Timing attack against modular exponentiation

Consider the following implementation of the modular exponentiation $C = M^D \bmod N$, where M is the plain text, C is the ciphertext, N is the public modulus, D is the w-bits secret exponent, and T is a temporary variable. The bits of D are numbered from $D(0)$ (most significant) to $D(w-1)$ (least significant).

```
1: $T \Leftarrow 1$
2: for $k = 0$ to $w - 1$ do
3:   $T \Leftarrow T^2 \bmod N$
4:   if $D(k) = 1$ then
5:     $T \Leftarrow (T \times M) \bmod N$
6:   end if
7: end for
8: return $T = M^D \bmod N = C$
```

The time taken by the modular square (line 3) and the modular multiplication (line 5) depends on the value of their operands. As we saw during the lectures, this implementation is not protected against the timing attack. A programmer rewrites this algorithm as follows:

```
1: $T \Leftarrow 1$
2: for $k = 0$ to $w - 1$ do
3:   $T \Leftarrow T^2 \bmod N$
4:   $U \Leftarrow (M - 1) \times D(k) + 1$
5:   $T \Leftarrow (T \times U) \bmod N$
6: end for
7: return $T = M^D \bmod N = C$
```

where U is a second temporary variable, and where the time taken by the operation of line 4 is constant. The programmer claims his algorithm is now protected against timing attacks. What do you think of this claim? In your answer clearly define your hypotheses. If you think the attack is not possible any more, explain in deep details why. Else, design a timing attack against this new implementation, clearly and carefully define your notations, and try to express your attack algorithm in a semi-formal way (pseudo-language) so that it is both complete and non ambiguous.