ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, SPRING 2023, assignments list # 8, 10.5.2023

1. The (obsolete but sometimes used) data encryption standard DES uses the so-called S-Boxes $S_1, ..., S_8$. These functions are given as lookup tables only. See, for example, `https://de.wikipedia.org/wiki/Data_Encryption_Standard`.

   Question: Is cache attack applicable against DES or its variants like 3DES? Explain the advantages and / or disadvantages of this techniques in this case.

   (A pseudocode of DES is given at `https://en.wikipedia.org/wiki/Data_Encryption_Standard`, where the function substitution means partitioning input to 6-bit strings and applying S_1 to the first string, S_2 to the second string, ...)

2. Out-of-order execution is one of the common techniques used to speed up computations on modern processors. The idea is that in parallel to the execution of the current instruction some number of subsequent instructions is executed as well. Their result may be incorrect (if for instance the result of the 1st instruction influences the input of the 2nd instruction) and all results are retired – their effects are discarded. However, in many cases, the results are correct and the processor may use them. This is a strategy for automatic parallelization of sequential algorithms.

   The idea of Meltdown attack: The goal is to read a byte x from the kernel of the operating system by a user process with no read rights to the kernel. An illegal access to the kernel results first in fetching the value x and then in interrupting the execution and erasing the result by the operating system.

   If the out-of-order mechanism is implemented, the user process may take the read value x and use it as an address of data to be fetched from an array owned by the user. This in turn may result in a cache miss and evicting some previous contents from the cache.

   Your task:

   (a) Analyze the pseudocode of Meltdown and explain how it works in detail (see paper `https://meltdownattack.com/meltdown.pdf`

   (b) Check for possibilities to learn more than one byte in this way. What are the problems?

3. A lookup table for AES could be stored in a different way, say the value $T_0(i)$ is not the ith entry in the lookup table, but at position $\bar{i}$, where $\bar{i}$ is the bit-reversal of i (i.e. if $i = [i_0, i_1, \ldots, i_k]$, then $\bar{i} = [i_k, \ldots, i_0]$.

   Questions: does it help against the cache attack? What are the differences?

/-/ Mirosław Kutyłowski