IT Security 2024/2025
Exercise Sheet 4
– Side Channel Attacks –

Dr. Jernej Tonejc

Publication: 31.10.2024
Deadline: 06.11.2024 10:00

Lightning Survey ⚡

Exercise 1 (Questions, 1+1+1+1+1 points)**.**
Create a file `answers.txt` and answer the following questions:

a) Which factors contribute to the Spectre/Meltdown bugs?

b) Suppose the exfiltration rate is 20 bits/hour. What could be the worthy targets?

c) Read about Flush+Reload and Prime&Probe. Explain the difference between the two methods.

d) Suppose we introduce Cache-Rollback to prevent spectre-type attacks by marking entries as uncached, if they were speculatively loaded and the load should not have happened. Would this work? What can attacker do in this case?

e) Consider the following code:

```c
#include "even_odd_lib.h"
int main(int argc, char** argv) {
    int secret = atoi(argv[1]);
    while (secret >>= 1) {
        if (secret & 0x1)
            odd();
        else
            even();
    }
    return 0;
}
```

Which side channels could exist?

Exercise 2 (Padding Oracle, 5 points)**.**
A server vulnerable to a Padding Oracle attack is available at `https://itsec.cs.uni-bonn.de/padorc/`. Read the instructions and write the script `padorc.py` to perform the attack. The pipeline for this task is limited to 10 minutes, so find an efficient solution.

Note: Brute Force is not efficient!
Note 2: The script might work a bit faster in the pipeline compared to your computer due to shorter request times.