# Software Vulnerabilities: Exploitation and Mitigation

—

# Lab 6

Alexandre Bartel

The report for the lab should consist of a single pdf file. Please use the following filename:

`lab6_FIRSTNAME_LASTNAME.pdf`

Send the report to alexandre.bartel@uni.lu with the following subject:

`MICS-SOFTVULN2019 Lab6 FIRSTNAME_LASTNAME`

Do not forget to put your name on the report itself. The deadline is April the $14^{th}$ 2019 at 23:59.

## 1 Lab6 (20 P.)

In this lab you will analyze how CFI is implemented in `clang`. Download `clang` as follows:

```
# apt-get install clang
```

### 1.1 CFI

Use the following sourc code:

```
#include <stdio.h>
#include <string.h>

int lt(int x, int y) {
  return x < y;
}
int gt(int x, int y) {
  return x > y;
}

int sort(int a[], int len, int (*f)(int, int)) {
  (*f)(a[len], a[len+1]);
```

```
  return 0;
}

int sort2(int a[ ], int b[ ], int len)
{
  sort( a, len, &lt );
  sort( b, len, &gt );
  return 0;
}

int main(int argc, char** argv) {
  int ia[10];
  int ib[10];
  sort2(ia, ib, argc);
  return 0;
}
```

---

**Question 1.1** Describe the source code. 3 P.

Compile the source code using `clang` without CFI:

```
$ clang -O0 -o default test.c
```

Compile the source code using `clang` with CFI:

```
$ clang -O0 -fsanitize=cfi -flto -fvisibility=hidden -o cfi test.c
```

**Question 1.2** Does gcc also support CFI? 1 P.

**Question 1.3** Describe all five options given to `clang` above. 5 P.

**Question 1.4** In the CFI version, there is the instruction `ud2` which is not in the non-CFI version. What is this instruction doing? 2 P.

You can disassemble the two versions using `objdump`:

```
$ objdump -d default > default.dump
$ objdump -d cfi > cfi.dump
```

You can `diff` the two versions using `vimdiff`:

```
$ vimdiff default.dump cfi.dump
```

**Question 1.5** What elements (instructions, functions, etc.) are in the CFI version and not in the non-CFI version. 2 P.

**Question 1.6** Explain how the added instructions check for CFI. Describre precisely under which conditions instruction `ud2` is executed. Drow the CFG for the C program above. 7 P.

## Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always properly cite your sources.