Fuzzing 101 - Step by step setup instructions

Instructor: didu@google.com / @0xdidu

Trainings:

- BlackHoodie GreHack, Nov 10, 2021
- GreHack, Nov 19, 2021

Requirements

- A recent Debian / Ubuntu machine (Ubuntu 20.04 for example). You can use either a virtual machine or your host directly, this does not matter for these exercises (it does for real fuzzing).
  Debian or Ubuntu on WSL on Windows is also a valid configuration.
- User in the sudoers list / root on the machine

Setup of AFL++ and clang

- Open a Linux terminal
- Execute:

```
sudo apt-get update
sudo apt-get install afl++ clang
```

More information on AFL++: https://github.com/AFLplusplus/AFLplusplus

Setup of libFuzzer

Installing clang includes libFuzzer (for any version > 6.0).
You could probably use an older version of clang if needed and install libFuzzer apart (but this has not been tested).
More information on LibFuzzer: https://llvm.org/docs/LibFuzzer.html#getting-started

Test of the setup

1. Verify that the commands afl-fuzz exists (for example by running `afl-fuzz -h`)
2. Verify that libFuzzer is installed. To do that, create the following file `test_fuzzer.cc`:

```
#include <stdint.h>
#include <stddef.h>
extern "C" int LLVMFuzzerTestOneInput(const uint8_t *data, size_t size) {
  if (size > 0 && data[0] == 'H')
    if (size > 1 && data[1] == 'I')
```

```
      if (size > 2 && data[2] == '!')
      __builtin_trap();
  return 0;
}
```

3. Open a Linux terminal and run the following commands:
   `clang++ -fsanitize=address,fuzzer test_fuzzer.cc`
   Expected output: nothing (and as a consequence no error).
   `./a.out`
   Expected output: the first line starts with "INFO: SEED: … ", then there are many lines, and the last line ends with a base64 string.

All this may look weird but the code snippet and the output of a.out will be explained during the class.

Troubleshooting:

- If clang++ is not found, this is probably because the symlink was not created. You can search clang++-<version> instead.
- Be careful to create a cc file (C++), not a c file.
- If the issue persists, you can contact me by email and describe the problem.

Setup the exercise folder

Whenever the source files are shared with you:

- Create a dedicated folder for the class
- Download the .c files shared with you for this class and move them to this directory.

🎉 **You're all set** 🎉

Follow up

If you have any follow up questions, you can send me an email on didu@google.com.