University of Potsdam

Institute of Computational Science

Lab 02

Software Security

Martin Stähr
M.Sc. Computational Science
754245

Max Schrötter
M.Sc. Computational Science
761220

Chenpo Hu
M.Sc. Computational Science
784196

June 28, 2018

1 Fuzzing Tool

Our fuzzing tool supply the two required modes `OVERFLOW` and `FORMATSTRING`.

We also supplied vuln.c: A simple C application that is vulnerable against both modes.

```
1 #include <string.h>
2 #include <stdio.h>
3 int main (int argc, char ** argv)
4 {
5     char temp[212];       // string to hold large temp string
6     strcpy(temp, argv[1]);   // take argv1 input and jam into temp
7     printf(temp);
8 }
```

The following output was created by our tool for the two modes.

1. FORMATSTRING

```
[mschroetter@surface lab02]$ ./tool.out vuln.out FORMATSTRING
Overflow detected of vuln.out, with the input:
 %4P5 %016lx %016lx %016lx %016lx %016lx %016lx %016lx %s
```

Figure 1: Brutefoce

For formatstring detection our tool creates an ether 32 bit or 64 bit random strings including characters that are not printable. We do it to get a better address coverage for the case that stack-protection is turned off. The printf filling string is also chosen depending on bit architecture. Currently our tool only allows formatstring detection on 32 bit and 64 bit architectures.

2. OVERFLOW

```
[mschroetter@surface lab02]$ ./tool.out vuln.out OVERFLOW
Signal Abort detected of vuln.out, with the input:
 OTY3geMxehcQHdBLdjqQSiLSvooSDF3sy2vPgimuzzkhNW30guQ8NC0i0oaE3d6CgCrwUO1uomMbiPbyk2G7FHpG5zk9NrM33dAY2CtqYf
Bh5NPpQwwvdVbjvwtjXfn1tY0vAtVyJxPOlFdcbKHpGTIbpbvnrSpUQppqTlZCTPqeuEqGp8552OhsZMPrFflvEKWx6V9ZLAdffEWEN1KPP
1hPN7gtmCY1nVytRIsCjGSylOd8PXXFZfvNmMgJofK
This is probably send by glibc Stackprotector
```

Figure 2: Overflow

The Overflow detection works by doubling the length of input each cycle. If the program exits with an error code out tool suspects that the tool is checking input length. For that reason the tool than increases the size by one from the last working input. We also test alway test different random strings to bypass other input checks.