

CSE 523S

Systems Security

Presentations & Semester Endgame

Spring 2022
Prof. Patrick Crowley

Plan for Today

- Fuzzing lab follow-up
- End of semester plans
- Presentation requirements & topics

Fuzzing Lab Follow-up

```
[03/29/22]seed@VM:Patrick$ ./so_gcc <
/tmp/findings/crashes/id\:000001\,sig\:11\,src\:000000\,op\:havoc\,rep\:12
8
[BEFORE] buffer_two is at 0xbfa3ed1c and contains 'two'
[BEFORE] buffer_one is at 0xbfa3ed24 and contains 'one'
[BEFORE] value is at 0xbfa3ed2c and is 5 (0x00000005)

[STRCPY] copying 2 bytes into buffer_two

[AFTER] buffer_two is at 0xbfa3ed1c and contains '??'
[AFTER] buffer_one is at 0xbfa3ed24 and contains '??'
[AFTER] value is at 0xbfa3ed2c and is -12582912 (0xff400000)
Segmentation fault
[03/29/22]seed@VM:Patrick$
```

Note that the input file has >100 bytes

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

int main(int argc, char *argv[]) {

    int value = 5;
    char buffer_one[8], buffer_two[8];
    char s[64];

    strcpy(buffer_one, "one");
    strcpy(buffer_two, "two");

    printf("[BEFORE] buffer_two is at %p and contains '%s'\n", buffer_two, buffer_two);
    printf("[BEFORE] buffer_one is at %p and contains '%s'\n", buffer_one, buffer_one);
    printf("[BEFORE] value is at %p and is %d (0x%08x)\n\n", &value, value, value);

    gets(s);
    printf("[STRCPY] copying %d bytes into buffer_two\n\n", strlen(s));
    strcpy(buffer_two, s);

    printf("[AFTER] buffer_two is at %p and contains '%s'\n", buffer_two, buffer_two);
    printf("[AFTER] buffer_one is at %p and contains '%s'\n", buffer_one, buffer_one);
    printf("[AFTER] value is at %p and is %d (0x%08x)\n", &value, value, value);

}
```

```
Terminal

american fuzzy lop 2.52b (bfd)

process timing
  run time : 6 days, 20 hrs, 16 min, 0 sec
  last new path : 0 days, 1 hrs, 49 min, 1 sec
  last uniq crash : 3 days, 19 hrs, 28 min, 18 sec
  last uniq hang : none seen yet

overall results
  cycles done : 0
  total paths : 611
  uniq crashes : 1
  uniq hangs : 0

cycle progress
  now processing : 275 (45.01%)
  paths timed out : 0 (0.00%)

map coverage
  map density : 1.03% / 2.70%
  count coverage : 2.66 bits/tuple

stage progress
  now trying : arith 32/8
  stage execs : 21.6k/68.3k (31.65%)
  total execs : 31.1M
  exec speed : 49.06/sec (slow!)

findings in depth
  favored paths : 176 (28.81%)
  new edges on : 252 (41.24%)
  total crashes : 2 (1 unique)
  total tmouts : 4 (4 unique)

fuzzing strategy yields
  bit flips : 334/4.29M, 70/4.29M, 13/4.29M
  byte flips : 5/535k, 1/89.8k, 2/94.0k
  arithmetics : 98/4.91M, 4/2.81M, 0/1.75M
  known ints : 2/336k, 14/1.79M, 6/3.30M
  dictionary : 0/0, 0/0, 14/2.43M
  havoc : 48/77.9k, 0/0
  trim : 12.69%/133k, 83.61%

path geometry
  levels : 3
  pending : 528
  pend fav : 138
  own finds : 610
  imported : n/a
  stability : 100.00%

[cpu:300%
```

Planned fuzzing HW: Our SEED VM takes 3 days to find the crash I expected!

Plan for Today

- Fuzzing lab follow-up
- End of semester plans
- Presentation requirements & topics

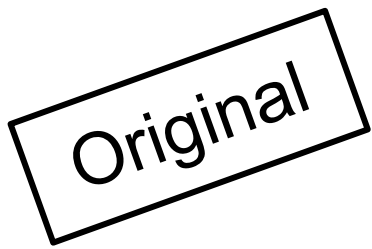
The next two weeks

Week 14		✓	+	⋮
Format String Vulnerabilities		✓		⋮
Apr 18 pre-recorded lecture (virtual class)		⊘		⋮
Apr 20 lab		⊘		⋮
Week 15		✓	+	⋮
Student presentations; wrap up		✓		⋮
Apr 25 Course wrap-up discussion		⊘		⋮
Apr 27 Student presentations & discussions due		⊘		⋮

There will be no more homework assignments this semester

Plan for Today

- Fuzzing lab follow-up
- End of semester plans
- Presentation requirements & topics



Presentations

- This is a 500 level class!
 - Find a topic, an incident or recent security news and present it to the class. (~15 minutes).
 - We will provide a list of topics to choose from.
 - Aim to make it a discussion and ask open-ended questions
 - 6 students will present in each lecture reserved for student presentations.
 - presentations will be pre-recorded and posted on discussion boards.

Updated

Presentations & Discussions

- **Presentations**

- **Due 10am Apr 27th – NO LATE WORK ACCEPTED! (See below)**
- Presentations will be recorded and posted in canvas discussion
- Find a topic and present it to the class. (no more than 10-15 minutes).
 - Apr 13 lecture includes a list of topic categories to choose from.
 - You must show your face in the video presentation
- Content your presentation must include
 - Clearly describe the details/findings/contributions of your topic
 - Explain why/what you find interesting or important about it
 - Pose 2 or more questions about it for follow up discussion

- **Discussions**

- **Due 11:30am Apr 27th – FIRM DEADLINE!**
- Each student must complete 2 follow-up peer reviews, answering a question from two different presentations.
 - You will automatically be assigned 2 discussions for peer review
 - Use the rubric to review and answer 2 questions
- A presentation can have at most 2 follow-ups. (Do not submit a third!)

Topic Categories

Academic papers

USENIX Security Symposium ([link](#))

IEEE Symposium on Security and Privacy ([link](#))

Security conference presentations

DEF CON ([link](#))

Blackhat ([link](#))

Vulnerability topic (e.g., from textbook not covered in class)

Race condition vulnerabilities

SQL injection

A hacking incident or breach

SolarWinds hack

Stuxnet

OKTA hack

You are not limited to these sample categories! You can choose any security topic of interest to you.

Any questions?