Report of
Programming Assignment 2: Fuzz Testing

By Piyusha Jaisinghani (UCFID - 4736715)

Table of Contents

Objective	3
Analysis	3
Design and Implementation	3
Implementation Steps	4
Execution	4
Results	6

Objective

Fuzz Testing is used to discover vulnerabilities in a code that processes potentially malicious input. The goal is to implement a mutation based fuzzer or fuzz tester for the image cross.jpg

The mutation-based fuzzer mutates the input cross.jpg, by making random changes and generate new test cases. Tracking down the bugs introduced in jpg2bmp by mutating the input image and feeding it to the jpg2bmp and save images that triggered bugs.

Analysis

The image bytes of the input image cross.jpg (808 bytes) is mutated. The mutated images are used as an input to jpg2bmp executable file to trigger manually introduced bugs in the file. The mutations are done by changing byte values to random values using the rand() function in c.

Design and Implementation

Programming Language used - C

Libraries included - stdio.h , stdlib.h, string.h, unistd.h, sys/wait.h

In this project the input image is stored in the input buffer and byte value mutations are done at 2000, 4000, 10000 iterations.

Observation:

- The bugs 4,5,7,8 were easy to generate by varying inputBuffer content at random index with random value. Tried multiple indices 40, 56 etc.

- I tracked down the random value at which bug 1 appears. It appears at index 48. Hence I added an if statement for this bug.

- Random index is generated using rand()%808, and random values were generated using rand() % 800 generating values from 1 to 800.

- Updating the code based on above two points, and when ran it for iteration 2000, bug 1 was detected 2 times and bug 3 only once along with bug 4,5,7,8. At 4000 iterations the count of bug-3 increased to 3.

- Multiple iterations are tested to find out the least number of mutations at which all 7 bugs appear. Memory usage and execution time increases with the number of iterations.

Implementation Steps

- In the code created two files inputFile for cross.jpg which reads the byte information of the image and outputFile to write the mutated.
- At every iteration the input image is mutated using the rand() function.
- After mutation of the input image, the command "./jpg2bmp test.jpg test.bmp" is executed to generate bmp files.
- Wait for the system response and if it responded with a bug then this bug information is read and if it is a valid bug from bugs 1-8, corresponding bug counter is incremented and image test#bugNumber is written to system.
- The latest mutated image that triggered the bug overwrites the previously generated same category bug and hence only one test-#bugNumber file is stored when program finishes.
- The crashCounter variable count the number of segmentation faults appeared during the execution, which leads to the crashed-* image creation.
- The output.txt stores how many times each bug was triggered and also the total number of segmentation faults occurred (response code 128+6 and 128+11).

Execution

- Created a folder structure in eustis for this assignment, **/home/net/pi846531/malwareproject/mutationfuzzer.**
- Copied the MutationFuzzer.c, jpg2bmp, cross.jpg in to the folder mutationfuzzer in eustis.

```
pi846531@net1547:~$ cd malwareproject/mutationfuzzer/
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
cross.jpg  jpg2bmp  MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

- Changed the permission to jpg2bmp using the following command:

$chmod u+x jpg2bmp

```
pi846531@net1547:~/malwareproject/mutationfuzzer$ chmod u+x jpg2bmp
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
cross.jpg  jpg2bmp  MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

- Converted cross.jpg to cross.bmp using the following command:

$./jpg2bmp cross.jpg cross.bmp

```
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp cross.jpg cross.bmp
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
cross.bmp   cross.jpg   jpg2bmp   MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

- Compiled the MutationFuzzer.c using the following command

gcc -o mutationfuz MutationFuzzer.c

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.u...
cross.bmp   cross.jpg   jpg2bmp   MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$ gcc -o mutationfuz MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
cross.bmp   cross.jpg   jpg2bmp   mutationfuz   MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

- Using the below command, executed the mutation fuzzer which copies the output to the file output.txt.

./mutationfuz >output.txt

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.uc...
cross.jpg   jpg2bmp   MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp  cross.jpg  cross.bmp
-bash: ./jpg2bmp : No such file or directory
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp cross.jpg cross.bmp
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
cross.bmp   cross.jpg   jpg2bmp   MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$ gcc -o mutationfuz MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
cross.bmp   cross.jpg   jpg2bmp   mutationfuz   MutationFuzzer.c
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./mutationfuz >output.txt
```

- The below screenshot depicts the completion of execution and list of all the bugs triggered and stored:

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu — 144×46
crashed image : ./crashed-165.jpg
Bug #2 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-166.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-167.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-168.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-169.jpg
pi846531@net1547:~/malwareproject/mutationfuzzer$ ls
crashed-100.jpg  crashed-129.jpg  crashed-157.jpg  crashed-31.jpg  crashed-5.jpg   crashed-88.jpg
crashed-101.jpg  crashed-12.jpg   crashed-158.jpg  crashed-32.jpg  crashed-60.jpg  crashed-89.jpg
crashed-102.jpg  crashed-130.jpg  crashed-159.jpg  crashed-33.jpg  crashed-61.jpg  crashed-8.jpg
crashed-103.jpg  crashed-131.jpg  crashed-15.jpg   crashed-34.jpg  crashed-62.jpg  crashed-90.jpg
crashed-104.jpg  crashed-132.jpg  crashed-160.jpg  crashed-35.jpg  crashed-63.jpg  crashed-91.jpg
crashed-105.jpg  crashed-133.jpg  crashed-161.jpg  crashed-36.jpg  crashed-64.jpg  crashed-92.jpg
crashed-106.jpg  crashed-134.jpg  crashed-162.jpg  crashed-37.jpg  crashed-65.jpg  crashed-93.jpg
crashed-107.jpg  crashed-135.jpg  crashed-163.jpg  crashed-38.jpg  crashed-66.jpg  crashed-94.jpg
crashed-108.jpg  crashed-136.jpg  crashed-164.jpg  crashed-39.jpg  crashed-67.jpg  crashed-95.jpg
crashed-109.jpg  crashed-137.jpg  crashed-165.jpg  crashed-3.jpg   crashed-68.jpg  crashed-96.jpg
crashed-10.jpg   crashed-138.jpg  crashed-166.jpg  crashed-40.jpg  crashed-69.jpg  crashed-97.jpg
crashed-110.jpg  crashed-139.jpg  crashed-167.jpg  crashed-41.jpg  crashed-6.jpg   crashed-98.jpg
crashed-111.jpg  crashed-13.jpg   crashed-168.jpg  crashed-42.jpg  crashed-70.jpg  crashed-99.jpg
crashed-112.jpg  crashed-140.jpg  crashed-169.jpg  crashed-43.jpg  crashed-71.jpg  crashed-9.jpg
crashed-113.jpg  crashed-141.jpg  crashed-16.jpg   crashed-44.jpg  crashed-72.jpg  cross.bmp
crashed-114.jpg  crashed-142.jpg  crashed-17.jpg   crashed-45.jpg  crashed-73.jpg  cross.jpg
crashed-115.jpg  crashed-143.jpg  crashed-18.jpg   crashed-46.jpg  crashed-74.jpg  jpg2bmp
crashed-116.jpg  crashed-144.jpg  crashed-19.jpg   crashed-47.jpg  crashed-75.jpg  mutationfuz
crashed-117.jpg  crashed-145.jpg  crashed-1.jpg    crashed-48.jpg  crashed-76.jpg  MutationFuzzer.c
crashed-118.jpg  crashed-146.jpg  crashed-20.jpg   crashed-49.jpg  crashed-77.jpg  output.txt
crashed-119.jpg  crashed-147.jpg  crashed-21.jpg   crashed-4.jpg   crashed-78.jpg  test-1.jpg
crashed-11.jpg   crashed-148.jpg  crashed-22.jpg   crashed-50.jpg  crashed-79.jpg  test-2.jpg
crashed-120.jpg  crashed-149.jpg  crashed-23.jpg   crashed-51.jpg  crashed-7.jpg   test-3.jpg
crashed-121.jpg  crashed-14.jpg   crashed-24.jpg   crashed-52.jpg  crashed-80.jpg  test-4.jpg
crashed-122.jpg  crashed-150.jpg  crashed-25.jpg   crashed-53.jpg  crashed-81.jpg  test-5.jpg
crashed-123.jpg  crashed-151.jpg  crashed-26.jpg   crashed-54.jpg  crashed-82.jpg  test-7.jpg
crashed-124.jpg  crashed-152.jpg  crashed-27.jpg   crashed-55.jpg  crashed-83.jpg  test-8.jpg
crashed-125.jpg  crashed-153.jpg  crashed-28.jpg   crashed-56.jpg  crashed-84.jpg  test.bmp
crashed-126.jpg  crashed-154.jpg  crashed-29.jpg   crashed-57.jpg  crashed-85.jpg  test.jpg
crashed-127.jpg  crashed-155.jpg  crashed-2.jpg    crashed-58.jpg  crashed-86.jpg
crashed-128.jpg  crashed-156.jpg  crashed-30.jpg   crashed-59.jpg  crashed-87.jpg
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

To remove the images named crashed-*.jpg the command **rm crashed*** is used.

Results

The below command is used to trigger a specific bug:

./jpg2bmp test-<bugnumber>.jpg test-out.bmp

The <bugnumber> is replaced with number 1-8.

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu — 144×23
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-1.jpg test-out.bmp
Bug #1 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-2.jpg test-out.bmp
Bug #2 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-3.jpg test-out.bmp
Bug #3 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-4.jpg test-out.bmp
Bug #4 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-5.jpg test-out.bmp
Bug #5 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-6.jpg test-out.bmp
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-7.jpg test-out.bmp
Bug #7 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$ ./jpg2bmp test-8.jpg test-out.bmp
Bug #8 triggered.
Segmentation fault (core dumped)
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

Empirical results:

Total Number of Bugs triggered: 7

Bug Number	Image File Name
Bug 1	test-1.jpg
Bug 2	test-2.jpg
Bug 3	test-3.jpg
Bug 4	test-4.jpg
Bug 5	test-5.jpg
Bug 7	test-7.jpg
Bug 8	test-8.jpg

Bug Number	Number of bug occurrences (2000 iterations)	Number of bug occurrences (4000 iterations)	Number of bug occurrences (10000 iterations)
Bug 1	2	3	3
Bug 2	5	8	24
Bug 3	1	3	10
Bug 4	62	123	310
Bug 5	6	15	53
Bug 7	19	40	91
Bug 8	87	164	371
Total Bug Occurrences	182	356	862
Total Segmentation Faults (including unqualified bugs)	198	385	931

Screenshot for 2000 iterations

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu — 135×41
crashed image : ./crashed-185.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-186.jpg
Bug #5 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-187.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-188.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-189.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-190.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-191.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-192.jpg
Bug #7 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-193.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-194.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-195.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-196.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-197.jpg
Segmentation fault (core dumped)
crashed image : ./crashed-198.jpg
pi846531@net1547:~/malwareproject/mutationfuzzer$ pico output.txt
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu —
  GNU nano 2.9.3                                     output.txt

 Number of segmentation faults: 198
 Bug1 occurrences: 2
 Bug2 occurrences: 5
 Bug3 occurrences: 1
 Bug4 occurrences: 62
 Bug5 occurrences: 6
 Bug6 occurrences: 0
 Bug7 occurrences: 19
 Bug8 occurrences: 87
```

Screenshot for 4000 iterations

apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu — 135×41

```
crashed image : ./crashed-372.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-373.jpg
Bug #7 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-374.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-375.jpg
Bug #5 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-376.jpg
Segmentation fault (core dumped)
crashed image : ./crashed-377.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-378.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-379.jpg
Bug #7 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-380.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-381.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-382.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-383.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-384.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-385.jpg
pi846531@net1547:~/malwareproject/mutationfuzzer$ pico output.txt
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu

```
 GNU nano 2.9.3                                              output.txt

 Number of segmentation faults: 385
 Bug1 occurrences: 3
 Bug2 occurrences: 8
 Bug3 occurrences: 3
 Bug4 occurrences: 123
 Bug5 occurrences: 15
 Bug6 occurrences: 0
 Bug7 occurrences: 40
 Bug8 occurrences: 164
```

Screenshot for 10000 iterations

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu —
Segmentation fault (core dumped)
crashed image : ./crashed-918.jpg
Segmentation fault (core dumped)
crashed image : ./crashed-919.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-920.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-921.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-922.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-923.jpg
Bug #4 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-924.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-925.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-926.jpg
Bug #7 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-927.jpg
Bug #7 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-928.jpg
Segmentation fault (core dumped)
crashed image : ./crashed-929.jpg
Bug #8 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-930.jpg
Bug #5 triggered.
Segmentation fault (core dumped)
crashed image : ./crashed-931.jpg
pi846531@net1547:~/malwareproject/mutationfuzzer$ pico output.txt
pi846531@net1547:~/malwareproject/mutationfuzzer$
```

```
apt305 — pi846531@net1547: ~/malwareproject/mutationfuzzer — ssh pi846531@eustis.eecs.ucf.edu
  GNU nano 2.9.3                                     output.txt

 Number of segmentation faults: 931
 Bug1 occurrences: 3
 Bug2 occurrences: 24
 Bug3 occurrences: 10
 Bug4 occurrences: 310
 Bug5 occurrences: 53
 Bug6 occurrences: 0
 Bug7 occurrences: 91
 Bug8 occurrences: 371
```