

Design

In the given problem, the executable “jpegconv” has certain vulnerabilities that can be triggered with certain value of image file. So what we need to do is to modify the exe. Such a way, that vulnerabilities can be exposed. The input given to it is .jpg file.

There are two techniques of fuzzy testing: mutation and protocol based. I am here is using mutation. For the solution, there are executable file named mfuzz.c which can trace the bugs.

To create the randomization techniques, I use srand(). The mfuzz.c code will prevent every mutated image file that causes crash to the “jpegconv” program. So there will occur n number of mutated image files for the same bug triggered n times during the fuzzing test.

Implementation

Any hexadecimal value in the image file can be changed and checked by providing input to jpegconv. If the modified version of the jpg invoke the BUG, then we need to save that .jpg file. To execute the idea, we randomly change the value.

Empirical results

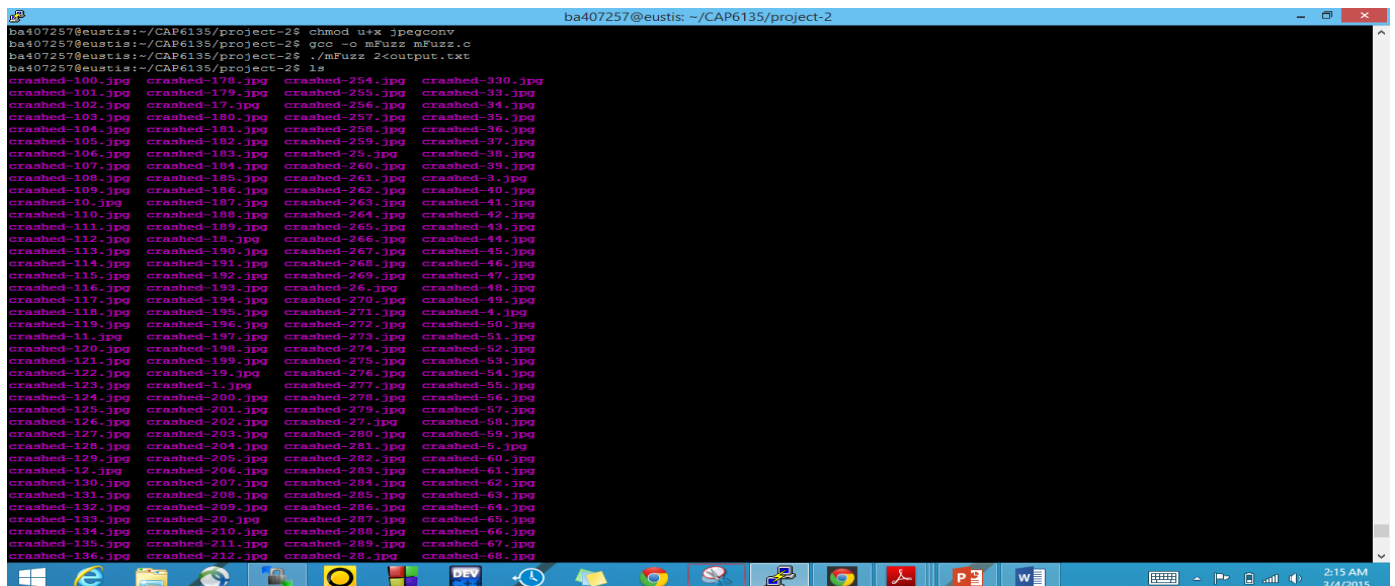
So it founds total 8 bugs(1,2,4,5,6,7,8,9) in the program. Main difference is, each of the newly created jpg file has only one byte different from the sample.jpg.

I have found all the test files and provided separately. Unfortunately I could not locate the exact file for Bug 2. So I have attached an output file screenshot and output file to show the BUG 2.

Total JPG created	329
No. of bugs found	Couldn't calculate properly, probably 150

Execution time near about 2 minute. Mostly all are BUG 5, and very few are other BUGs found in count.

Screenshot



Images - ba407257@eustis.eecs.ucf.edu - WinSCP

LocalMarkFilesCommandsSessionOptionsRemoteHelp

SynchronizeQueueTransfer Settings: Default

ba407257@eustis.eecs.ucf.eduNew Session

Desktopproject-2Find Files

UploadDownloadEditProperties

ba407257@eustis: ~/CAP6135/project-2

ba407257@eustis: ~/CAP6135/project-2

```
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-1.jpg
BUG 1 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-4.jpg
BUG 4 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-5.jpg
BUG 5 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-6.jpg
BUG 6 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-7.jpg
BUG 7 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-8.jpg
BUG 8 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$ ./jpegconv -ppm -outfile foo.ppm test-9.jpg
BUG 9 TRIGGERED
Segmentation fault
ba407257@eustis:~/CAP6135/project-2$
```

File Name	Ext	Size	Changed	Rights	Owner
test-1.jpg		35,264 B	3/3/2015 8:58:20 PM	rw-rw-r--	ba4072...
test-4.jpg		560 KiB	3/3/2015 8:54:10 PM	rw-rw-r--	ba4072...
Fuzz.c		7,775 B	3/4/2015 2:12:32 AM	rw-rw-r--	ba4072...
output.txt		1,566 B	3/4/2015 12:29:37 AM	rw-rw-r--	ba4072...
template.format		2,548 B	3/3/2015 8:54:10 PM	rw-rw-r--	ba4072...
template.jpg		5,155 B	3/3/2015 8:54:10 PM	rw-rw-r--	ba4072...
test.jpg		5,155 B	3/4/2015 2:13:46 AM	rw-rw-r--	ba4072...
test-1.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...
test-4.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...
test-5.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...
test-6.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...
test-7.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...
test-8.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...
test-9.jpg		5,155 B	3/3/2015 4:52:15 PM	rw-rw-r--	ba4072...

0 B of 41,240 B in 0 of 8

0 B of 874 KiB in 0 of 15

SFTP-36:57:04