PNG-Fuzzing with JQF

Paul Kalz, Marwin Linke, and Sebastian Schatz

Humboldt University of Berlin, Germany

Abstract. Fuzzing is a dynamic testing technique used to discover bugs and security issues in programmes and software systems. It is an essential technique of software testing and security assurance. There are different fuzzing strategies ranging from simple mutation-based techniques to more advanced generator-based techniques, but they all have in common that they operate by automatically injecting a lot of different data into a target program's inputs to uncover bugs, unforeseen behaviors, system failures or vulnerabilities.
The paper aims to summarize programming of a generator-based PNG fuzzer in JQF, with the target library of our fuzzer being PNGJ. Firstly, the paper provides a brief overview of the concept of usage of PNG and its specifications, as well as the security of PNG files. Furthermore, an overview regarding used tools and the process, had been provided. The implementation of the PNG generator is shown in detail and an overview of the implementation of the fuzz driver has been provided. Finally, the paper provides evaluation and discussion of the results. Keywords: PNG, Fuzzer, JQF

Keywords: PNG · Fuzzing · JQF.

1 Background on the File Format PNG

1.1 Overview

History The idea of PNG and its development started in January 1995 after the compression algorithm LZW, used in GIF (Graphics Interchange Format), was patented. Authors of GIF-supporting software had to pay to use it since December 1994. PNG stands for Portable Network Graphics and was designed to be better, smaller and more extensible than GIF. PNG is free and supposed to be the successor of GIF.

On the 1st of October 1996, PNG spec 1.0 was approved as W3C Recommendation and on the 15th of January 1997, PNG spec 1.0 was released as Informational RFC 2083 (IETF) [1]. In 2004, PNG was published as an ISO/IEC 15948 standard.

Use Cases PNG is a raster-graphics file format, which allows lossless data compression and supports RGB and RGBA colors, as well as grayscale images. At default PNG does not allow animated graphics and is mostly used on the

Internet for transferring images and pictures, for example it is often used for icons and buttons on websites. Since PNG does not support other color spaces than RGB/RGBA, it is not used for professional-quality print graphics or professional photographs.

1.2 Input Specification

PNG is specified as an Informational RFC 2083 (IETF) and has a formal specification as an ISO/IEC 15948 standard. This section provides a brief overview of the structure of PNG, more details are in section 3 Generator. Based on the structure of PNG, its byte streams can be broken down into chunks. There are different types of chunks with different information in them [11]. 3 types of chunks are critical for every PNG: `IHDR`, `IDAT` and `IEND`, that means that they have to appear. There is another chunk that is critical for color type 3 called `PLTE`. Every PNG file starts with the 8-byte signature `89 50 4E 47 0D 0A 1A 0A`; and each byte has its own purpose [3].

Example An example for a very small PNG image, displaying a single red pixel, is the following sequence of bytes:

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00 01 00 00
00 01 08 02 00 00 00 90 77 53 DE 00 00 00 0C 49 44 41 54 08 D7 63
F8 CF C0 0000 03 01 01 00 18 DD 8D B0 00 00 00 00 49 45 4E 44 AE
                                  42 60 82
                              PNG IHDR IDAT IEND
```

Signature

- `89` distinguishes PNG files on systems that expect the first two bytes to identify the file type uniquely.
- `50 4E 47` stands for PNG in ASCII, so that if a person opens a PNG file in a text editor the first word is PNG.
- `0D 0A` catches bad file transfers that alter newline sequences.
- `1A` is a byte that stops the display of the file with DOS.
- `0A` checks for the inverse of the CR-LF translation problem.

Image Header (`IHDR`)

- `00 00 00 0D` This chunk has 13 bytes of content.
- `49 48 44 52` This is an IHDR chunk (chunk type in ASCII).
- `00 00 00 01` The image is 1 pixel wide.
- `00 00 00 01` The image is 1 pixel high.
- `08` 8 bits are used per channel.
- `02` Color type 2 is used.
- `00` The compression method is 0.
- `00` The filter method is 0.
- `00` No interlacing is used.
- `90 77 53 DE` The CRC of the chunk's type and content.

Image Data (`IDAT`)

- `00 00 00 0C` This chunk has 12 bytes of content.
- `49 44 41 54` This is an IDAT chunk (chunk type in ASCII).
- `08` is a Deflate compression method using a 256-byte window.
- `D7` is a ZLIB FCHECK value, which indicates, that no dictionary and the maximum compression algorithm is used.
- `63 F8 CF C0 00 00` A compressed Deflate block using the static Huffman code (this sequence makes the pixel red).
- `03 01 01 00` is the ZLIB check value.
- `18 DD 8D B0` the CRC of the chunk's type and content.

Image End (`IEND`)

- `00 00 00 00` This chunk has 0 bytes of content.
- `49 45 4E 44` This is an IEND chunk (chunk type in ASCII).
- `AE 42 60 82` The CRC of the chunk's type and content.

1.3 Security

Over the previous years, several security issues had been detected with PNG files. Libpng is the official PNG reverence library and has a good documentation for fixed security vulnerabilities [2]. Currently, 47 vulnerabilities are known and fixed for Libpng. These vulnerabilities range from less important ones like an error message when opening a PNG to very serious ones, where attackers can execute arbitrary code. The most dangerous vulnerability is documented in CVE-2014-9495, as a Heap-based buffer overflow in the `png_combine_row` function in libpng before 1.5.21 and 1.6.x before 1.6.16. Where when running on 64-bit systems, might allow context-dependent attackers to execute arbitrary code via a "very wide interlaced" PNG image. That vulnerability basically allowed attackers to install malware on the device that opened the PNG.

2 Implementation

2.1 Tools

JQF The coverage-guided testing platform for Java named JQF, developed by R. Padhye, C. Lemieux and K. Sen, is designed for *practitioners*, who want to find bugs in Java programs, as well as for *researchers*, who wish to implement new fuzzing algorithms [4]. As for our project, we used JQF to implement a fuzzing generator based on the file format PNG, which is tested by a driver directly in JQF.

PNGJ To test our fuzzer we chose PNGJ, which is a pure, open-source Java library for high-performance reading and writing of PNG images [6]. Especially the reading capability of PNGJ was tested by the fuzzer.

Java Standard Library PNG files use compression algorithms [8] as well as multiple checksum algorithms, which are all provided by the Java standard package `java.util.zip` [9]. The fuzzer is dependent on the correctness of those algorithms and therefore uses this library to ensure reliable results instead of implementing the algorithms itself.

2.2 Process

To implement the PNG fuzzer and test the library, a generator and driver class needed to be written. The generator is a self-contained class, which is called by JQF and returns a specified data type. In our case, the generator returns `PngData`, which wraps a byte array of a functional PNG file. Next, the fuzz driver receives the `PngData`, which in turn is processed by PNGJ. The fuzz driver itself can be designed flexibly to test multiple functionalities in a library. This process is automatically repeated; each time JQF uses the guidance algorithm Zest [5] to guide the randomized seeds from the generator in a more beneficial direction.

3 Generator

3.1 Chunk Structure

The byte stream of PNG images can be broken down into chunks, where each one contains certain information and serves a concrete purpose [11]. A chunk is marked by its uniform structure found in the header and trailer surrounding its content.

Table 1: Byte strucure of a chunk [10].

Chunk length	**Chunk type**	**Chunk data**	**CRC**
4 bytes	4 bytes	*Length* bytes	4 bytes

As shown in table 1, each chunk consists of 4 parts [10]. The *chunk length* refers to a 4-byte unsigned integer giving the number of bytes in the content field of that chunk, it doesn't include the length of the chunk type nor the CRC checksum at the end. The *chunk type* is always represented by 4 characters each 1 byte long to uniquely identify each type of chunk. It uses capitalization to imply information about the chunk. The *chunk content* is the main part of each chunk and contains various amounts of data. The *CRC32* is a well-known checksum algorithm, which uses 32 bits. It includes the chunk type and content but not the length field.

We encapsulated this common structure in the class called `ChunkBuilder`. After generating the contents of a chunk, we simply call:

```
ChunkBuilder.constructChunk(chunkType, chunkContent)
```

with the according type and content as byte arrays or streams and receive a complete chunk, which then is concatenated with other chunks to form a PNG file.

3.2 PNG Structure

Chunks follow ordering constraints to form PNG files. There are 4 critical chunks (critical means that the chunk must appear), which determine the ordering of optional chunks.

Every PNG file must begin with a fixed 8-byte signature and the first chunk named `IHDR`. The `IHDR` stores important image information which are commonly accessed by its following chunks. The end of each PNG file is marked by the `IEND` chunk, which has no content but still a chunk header and trailer as mentioned in 3.1.

Between those chunks, the critical chunks `IDAT` and `PLTE` are found which hold information about the image data such as pixel color values as well as a color palette for indexed images. Further optional chunks are sorted into the space before `PLTE`, between `PLTE` and `IDAT` or after `IDAT`. For the exact ordering constraints, please refer to the PNG specifications [11].

Parameters The generator needs to keep track of which chunk is generated and then order them correctly. For that case, every chunk uses a boolean flag to indicate if it is used or not, which is enabled in `initializeParameters()`.

Furthermore, the generator stores parameters about information that is shared between chunks, for example, the bit-depth, the color type and the image size. Before each run, the generator resets its parameters with `resetParameters()`.

Optional Chunks In this section, a short overview will be given to explain which optional chunks [11] our generator can generate.

Color Space Information `cHRM`, `gAMA`, `iCCP`, `sBIT`, `sRGB` are chunks that are used to specify color space information, they define how the image is supposed to be displayed. They must appear before the `PLTE` chunk.

Miscellaneous Information After Palette `bKGD`, `hIST`, `tRNS` are chunks to convey miscellaneous information about the image mainly related to the palette, such as the background color, frequency of colors in a palette or transparency values in a palette. They all appear between the `PLTE` and `IDAT` chunk.

Miscellaneous Information `pHYs`, `sPLT` are also chunks to convey miscellaneous information but can appear anywhere between the `IHDR` and `IDAT` chunk.

Textual Information `tIME`, `iTXt`, `tEXt`, `zTXt` are chunks to hold textual information about the image such as the time the image was last modified or information about the title, author and more. They don't have any ordering constraints.

3.3 IHDR

The `IHDR` chunk, short for image header, stores critical information about the image and determines what type of image the fuzzer generates. It includes the *image width*, *image height*, *bit-depth* (also called *bits per channel*), *color type*, *compression method*, *filter method* and an *interlace boolean*. The generator randomizes these parameters, except for the compression method and filter method: At present, only method 0 is defined for both in the `IHDR` chunk [11]. The generator still uses different compression methods as well as filter methods, but they are instead defined in their respective chunks.

Image Size The randomized *image width* and *image height* can take on values between 1 and 10 pixels each, going larger than 10 pixels didn't seem to affect the number of covered branches. The size of up to 8 pixels contributes to the behaviour of interlacing (See section 3.5), thus greatly increasing the coverage.

Bit-depth The *bit-depth* defines the number of bits per channel. A channel refers to a single color value or alpha value. The bit-depth is directly dependent on the color type and only certain values are allowed to be used (See table 2).

Table 2: Allowed bit-depths per color type [11].

Color type	**Allowed bit-depths**	**Interpretation**
0	1, 2, 4, 8, 16	Grayscale
2	8, 16	RGB
3	1, 2, 4, 8	Indexed
4	8, 16	Grayscale with alpha
6	8, 16	RGB with alpha (RGBA)

Color Types The *color type* determines the number channels per pixels and the structure how they are stored. Grayscale images (color type 0) consist of 1 channel per pixel, RGB images (color type 2) have 3 channels for red, green and blue. Both of these color types can include an alpha channel, which in turn makes them grayscale with alpha (color type 4) or RGBA (color type 6) [14].

Indexed images (color type 3) are used to decrease memory space and feature a palette in the `PLTE` chunk. Instead of assigning each pixel multiple values for their respective channels (for example 3-bytes for an RGB image with a bit-depth of 8), indexed pixels only have 1 channel with the size of the bit-depth and hold an index to the palette. The palette stores up to 256 entries (dependent on the bit-depth), each a 3 byte series of values representing red, green and blue. The main advantage comes from an image having the same colored pixel multiple times, which doesn't need to be stored separately in indexed images.

As for the exact implementation, the generator first selects a random color type, then randomly chooses one of the allowed bit-depths and stores both information as parameters. Furthermore, the number of channels is determined based on the color type. The flags of certain chunks are enabled, some optional chunks are enabled by chance, whereas chunks like the palette are mandatory for indexed images. An example of an optional chunk would be the `tRNS` one, which adds corresponding alpha values for entries in the palette.

3.4 IDAT

The `IDAT` chunk is used to store the pixel data of an image, which is first filtered and then compressed [11] by a *deflate compression* [8], which is a derivative of the *LZ77 compression* used in `zip`, `gzip`, `pkzip` and related programs [12].

The generator uses the standard library `java.util.zip` which already implements the exact compression algorithm used for PNG files. It also includes an additional checksum, named *Adler32*, which appends to the compressed data.

Image Data The raw image data is a series of bytes which is divided into scanlines (rows) and pixels [14]. Each scanline starts with a filter byte, which represents the filtering method used for that scanline.

The generator calculates the number of scanlines and pixels based on the image width and height. After the filter byte, each scanline filters and appends pixels with randomized color channels accordingly. The size and number of channels are based on the color type and bit-depth.

Filtering There are five different filtering methods, whereas an empty byte (0) represents no filtering. Methods 1 to 4 indicate the use of *Sub*, *Up*, *Average* or *Paeth filtering*. The reason to use filtering is to represent the color values relative to their neighbouring pixels, this allows the deflate algorithm to compress patterns which are found relatively between pixels. The generator implements the filtering algorithms following the pseudo-code written in the specification [13].

3.5 Interlacing

Interlacing is a procedure to render an image over multiple passes. It starts with a low resolution and increases with each pass until the complete image is shown. This allows large PNG files to be rendered smoothly instead of waiting for the

complete image to be rendered at once. Interlacing is done by including multiple `IDAT` chunks in the PNG file, each one representing one pass of the rendering procedure. The first `IDAT` chunk only contains 1/64 of the pixels, the next one contains 1/32, then 1/16 and so on. The final, seventh pass contains the complete image. Which pixels are included is based on an 8-by-8-map of pixels [14].

The generator implements interlacing by generating multiple `IDAT` chunks with a lower image width and height, this doesn't represent true interlacing since each pass uses randomized pixels but it doesn't hinder most PNG readers, rendering the image regardless and covering branches.

3.6 Other Chunks

All of the critical chunks have been explained to this point but the generator also implements optional chunks. This section will not provide more information about the exact implementation of the rest, because optional are primarily used to store additional information in an image. This is easily implemented by filling those chunks with random bytes, adhering to the size and structural constraints as specifeid [11].

4 Fuzz Testing

4.1 Fuzz Driver

As for the fuzz driver, we decided to use code samples, provided directly by *PNGJ* itself [7], and combine them to test multiple functionalities. The largest contribution to the covered branches came by simply reading the PNG data, this covers all chunks, albeit superficially. To test for detailed aspects of the library we also included a pipeline that changes the PNG image depending on its color type and rereads the data in every step. The reason why we decided to make the driver dependent on the color type is that most functionalities are only applicable to certain color types, generating more valid inputs.

In the first step, the fuzz driver checks for indexed images that use a palette and converts them to true color images that use RGB or RGBA. In the second step, all converted images and images that were generated with true color by default are desaturated and converted to grayscale. Lastly, all converted images and images that were generated with grayscale by default are tested by mirroring the image.

Although this approach tests multiple functionalities, it is still far from covering all functionalities. It would need a very detailed fuzz driver to cover everything, which would pose its own challenge and lie outside the scope of this project.

4.2 Guidance

JQF also offers the possibility to alter its guidance properties, this is a useful aspect of fuzzing. However, we decided to not use it and stick to the default guidance settings.

PNG is a very interesting data format when it comes to fuzzing. The general idea of fuzzing is to generate random data that tries to cover most of the functionality of a program. In contrast, the precise specifications of PNG files make this a difficult task. Due to many checksums, compression algorithms and concrete identifiers, PNGs are rare to come across purely randomly. Practically every byte must be at its exact location with its exact, intended value. The explicit nature of PNGs may offer approaches like grammar fuzzing to be successful, whereas mutational fuzzing would pose a great challenge.

5 Evaluation

5.1 Experiments

To evaluate the efficiency of our implementation, we fuzzed the *PNGJ*-libary with the following four fuzzers using our fuzz driver:

- A **Complete Fuzzer**, which uses the full capability of our generator to correctly generate all critical and optional chunks as specified [11].
- A **Random Fuzzer** as a baseline, which generates random chunks in which only the chunk types and the CRC checksums of the chunks are calculated correctly.
- A **Probable Fuzzer** a version of our random baseline that additionally generates a correct IHDR and a partially correct IDAT chunk. The structure of the PNG files is therefore correct at least in the cirtical chunks.
- A **Simple Fuzzer** a simplified version of our Complete Fuzzer, which contains only IHDR, IDAT, PLTE and IEND chunks, all colour types, only bit-depth of 8, default compression, no interlacing and no filtering. This fuzzer therefore generates only correct PNG files.

Every fuzzer except the Simple Fuzzer is also able to generate optional chunks, albeit by chance.

We tested PNGJ with each fuzzer 10 times, with each repetition taking one hour. All experiments were executed on a Windows 10 system using a GTX 1060 6 GB GPU, a Intel i5 7600k CPU with 16 GB DDR4-3200 RAM. The experiments were run sequentially.

5.2 Results

We did not find any bugs or crashes during our tests, so we were only able to analyse the coverage of the fuzzers.

In the following diagrams, the blue graph always belongs to the Complete Fuzzer, the red graph to the Probable Fuzzer, the green graph to the Simple Fuzzer, and the black graph to the Random Fuzzer.

Total Coverage

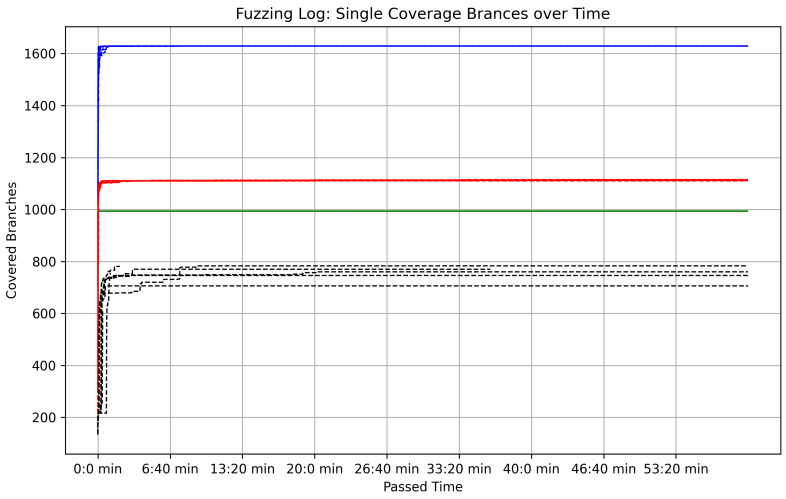

Fig. 1: Coverage for each repetition over time

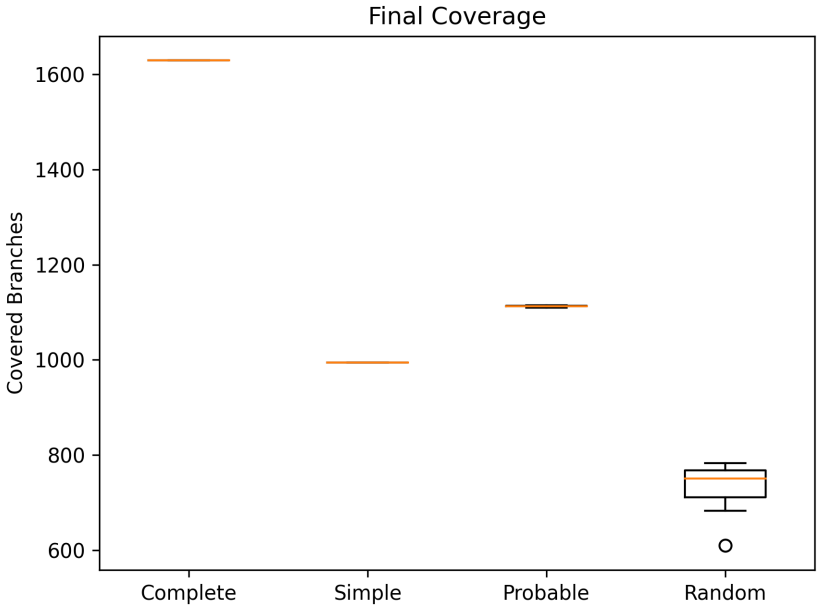

Fig. 2: Final Coverage

With our Complete Fuzzer, we managed to cover 1629 branches in every repetition. The Probable Fuzzer covered an average of 1112.9 branches. The Simple Fuzzer covered 994 Branches in every repitition. And the Random Fuzzer covered an average of 732,2 branches.

The number of covered branches for the Complete Fuzzer and the Simple Fuzzer did not change during the runs. This is why Figure 2 does not show any variance in the final coverage. The coverage of the Probable Fuzzer fluctuated slightly between 1110 and 1115 branches during the test runs. The coverage of the Random Fuzzer varied significantly more from 610 to 783 branches. It can also be observed that the fuzzers find a lot of new branches in the first minute and that the coverage almost stops to increase after that.

Table 3: Coverage for each fuzzer.

Fuzzer	**Average coverage**	**Average valid coverage**
Complete Fuzzer	1629	1629
Random Fuzzer	732.2	0
Probable Fuzzer	1112.9	1053
Simple Fuzzer	994	994

Valid Coverage

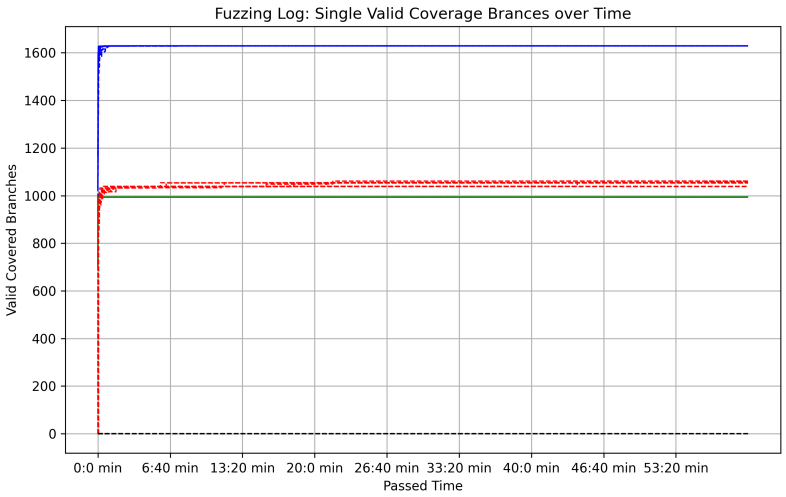

Fig. 3: Valid Coverage over time

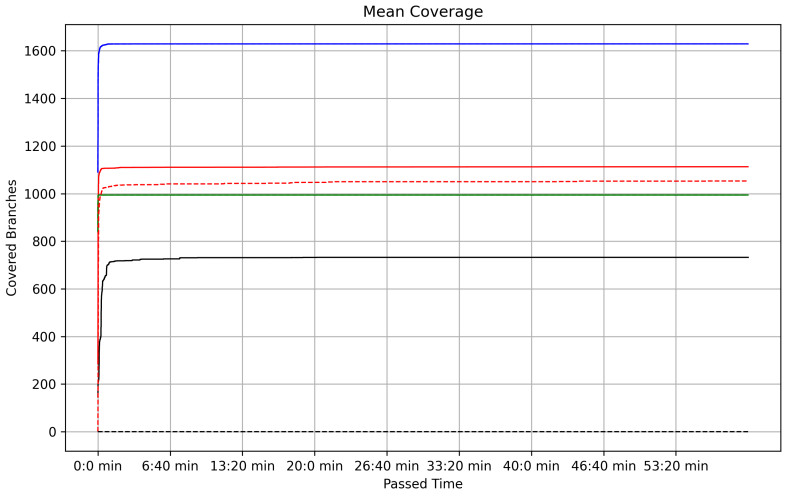

Fig. 4: Mean Coverage over time (dotted graphs are valid coverage)

The valid coverage of the Complete Fuzzer and the Simple Fuzzer is identical to their total coverage. The Probable Fuzzer covers between 1038 and 1061 valid branches. That is slightly less than its total coverage. The Random Fuzzer had no valid coverage in our tests.

We checked the statistical significance of the differences in coverage using Mann-Whitney U tests. However, it is already clear from the figures that there is no overlap between the measurements of the fuzzers and that the differences are therefore significant.

6 Result Discussion

6.1 Discussion

As expected, the Complete Fuzzer provides the greatest coverage. As it contains many optional chunks and features, it can utilise many of PNGJ's functions. This becomes particularly clear when it is compared with the Simple Fuzzer, which covers a much smaller number of branches due to its limited options. The Probable Fuzzer has decent coverage for its relatively low implementation effort. However, due to the complexity of a PNG file, it is very unlikely to randomly generate one of the options that would enable even higher coverage. The same applies to the Random Fuzzer.

The fact that the fuzzers reach their maximum coverage after about a minute may be explained by the limited complexity of the PNGJ library as well as our

test driver. The final coverage of the Probable and Random Fuzzers varies between runs, as sometimes options are found randomly that lead to more coverage and sometimes not. With the Complete and Simple Fuzzer, on the other hand, the structure is more strictly predefined, so it is more likely to generate all possible options, which seems to have happened during our runs.

When testing the Random Fuzzer, a Heap Error sometimes occurred which caused our fuzzing run to crash. We have not yet been able to find the cause of this error.

The valid coverage of the Complete Fuzzer and the Simple Fuzzer is identical to their total coverage, because these two Fuzzers only generate valid PNG-files. The valid coverage of the Probable Fuzzer is on average slightly below its total coverage, which should be due to the fact that this fuzzer can generate all critical chunks correctly. The random fuzzer has no valid coverage, as it is very unlikely to generate a correct PNG file at random.

6.2 Conclusion

Our generator creates valid PNG files that can contain all critical and optional chunks. This gives us significantly higher total and valid coverage on our fuzzing targets than simpler fuzzers. PNG is a relatively complex file format in which there are many dependencies between individual components. Therefore, a PNG generator needs a fairly fixed structure to generate valid files. Generating PNGs is thus not efficient with simple fuzzers that are largely based on chance.

6.3 Future Work

Our generator could be tested on other more complex fuzzing targets. In addition, the JQF guidance could be adapted to possibly deliver better results with our generator.

References

1. Thomas Boutell. 1997. RFC Editor, PNG (Portable Network Graphics) Specification Version 1.0
2. Libpng, Security vulnerabilities, CVEs, https://www.cvedetails.com/vulnerability-list/vendor_id-7294/Libpng.html?page=1&order=3&trc=47&sha=20a26d14531b8eff223b0769a2834502ea917ecf
3. Libpng, Rationale, http://www.libpng.org/pub/png/spec/1.2/PNG-Rationale.html
4. Rohan Padhye, Caroline Lemieux, and Koushik Sen. 2019. JQF: Coverage-Guided Property-Based Testing in Java. In Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA '19), July 15–19, 2019, Beijing, China. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3293882.3339002
5. Rohan Padhye, Caroline Lemieux, Koushik Sen, Mike Papadakis, and Yves Le Traon. 2019. Semantic Fuzzing with Zest. In Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'19), July 15–19, 2019, Beijing, China. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3293882.3330576

6. PNGJ GitHub-Page, https://github.com/leonbloy/pngj?tab=readme-ov-file
7. PNGJ Samples,
   https://github.com/leonbloy/pngj/tree/master/src/test/java/ar/com/hjg/pngj/samples
8. RFC 1951, Deflate Compressed Data Format Specification,
   https://datatracker.ietf.org/doc/html/rfc1951
9. Package `java.util.zip`,
   https://download.java.net/java/early_access/valhalla/docs/api/java.base/java/util/zip/package-summary.html
10. Libpng: File structure,
    http://www.libpng.org/pub/png/spec/1.2/PNG-Structure.html
11. Libpng: Chunk specification,
    http://www.libpng.org/pub/png/spec/1.2/PNG-Chunks.html
12. Libpng: Deflate algorithm,
    http://www.libpng.org/pub/png/spec/1.2/PNG-Compression.html
13. Libpng: Filtering,
    http://www.libpng.org/pub/png/spec/1.2/PNG-Filters.html
14. Libpng: Data representation,
    http://www.libpng.org/pub/png/spec/1.2/PNG-DataRep.html