Reverse Engineering

Amir Vspades
vegaspades@gmail.com

Sasan Rocky
s.rocky@farhost.net

Abstract

This study compares the Forward Engineering and Backward Engineering (also known as Reverse Engineering). In addition, some tools related to such field have been reviewed.

1 Introduction

Reverse Engineering, also called *Backward Engineering*, is the process by which a man-made object is de-constructed to reveal its designs, architecture, or to extract knowledge from the object [1]. Reverse Engineering is applicable in the fields of *Software Re-Engineering*.

Software Re-Engineering is the examination and alteration of a system to reconstitute it in a new form. The principles of Re-Engineering when applied to the software development process is called software re-engineering. It affects positively at software cost, quality, service to the customer and speed of delivery [2]. Figure 1 illustrates the procedure of Software Re-Engineering.

2 Reverse Engineering Tools

All tools[1] that are useful in such field, could be categorized into the following groups:

1. **Hex Editor**: A hex editor (or binary file editor or byte editor) is a computer program that allows for manipulation of the fundamental binary data that constitutes a computer file [3].
2. **Debugger**: A debugger or debugging tool is a computer program used to test and debug other programs (the "target" program) [4].
3. **Disassembler**: A disassembler is a computer program that translates machine language into assembly language [5].
4. **Decompiler**: A decompiler is a computer program that takes an executable file as input, and attempts to create a high level source file which can be recompiled successfully [6].
5. **Patcher**: A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it [7]. After altering the $.EXE$ file, we could use a patcher to generate a new modified $.EXE$ from the original one.
6. **Compressor**: A file archiver is a computer program that combines a number of files together into one archive file, or a series of archive files, for easier transportation or storage. File archivers may employ lossless data compression in their archive formats to reduce the size of the archive [8].
7. **Analyzer**: Static program analysis is the analysis of computer software that is performed without actually executing programs, in contrast with dynamic analysis, which is analysis performed on programs while they are executing [9].
8. **Monitoring Tools** including:
   (a) Registry Monitor
   (b) File Monitor
   (c) Port Monitor
   (d) Network Monitor
   (e) Process Explorer
9. **Protector**: In software development, obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand [10].

2.1 Hex Editor

The following tools could be recognized as Hex Editors:

1. Hiew [2]
2. WinHex [3]
3. Hackman Suite [4]
4. Hex Workshop [5]

2.2 Debugger

The following tools could be recognized as Debuggers:

1. NuMega SoftICE [6]
2. WinDbg [7]
3. OllyDbg [8]

[1] Some of the tools mentioned in this article are archived and accessible via this link: http://mega.nz

[2] http://www.hiew.ru/
[3] http://www.winhex.com/winhex/
[4] https://www.technologismiki.com/prod.php?id=31
[5] http://www.hexworkshop.com/
[6] https://archive.org/details/NuMega_SoftIce_Windows_3.2
[7] https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools
[8] http://www.ollydbg.de/

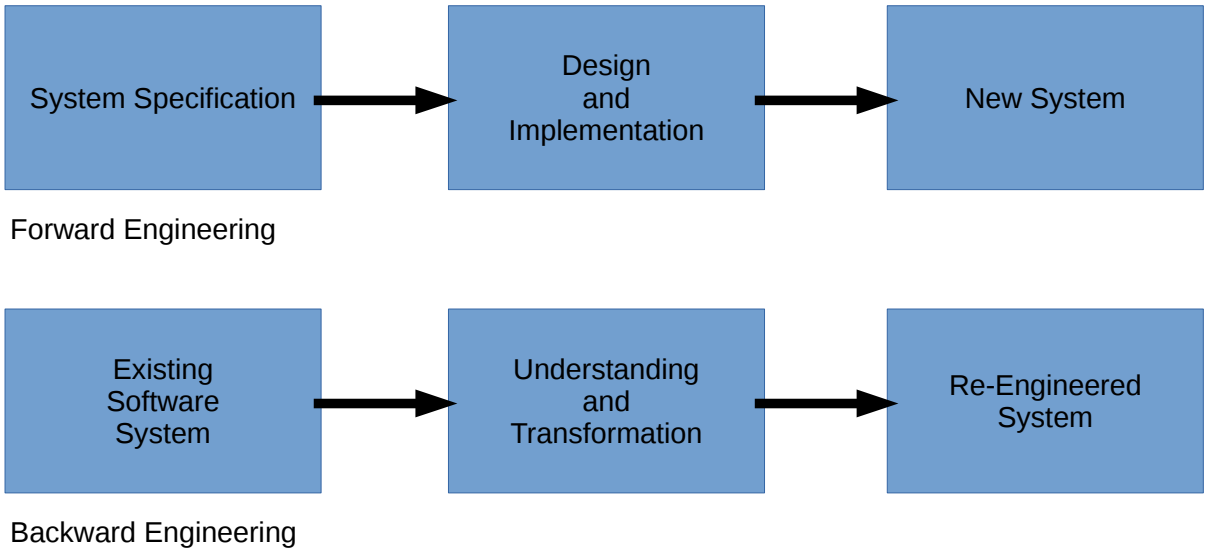

Figure 1: Forward Engineering vs. Backward Engineering

4. IDA Pro [9]

2.3 Disassembler

The following tools could be recognized as Disassemblers:

1. WinDasm [10]
2. ilDasm [11]

2.4 Decompiler

The following tools could be recognized as Decompilers:

1. JAD [12]
2. Reflector [13]
3. SWF Decompiler [14]

2.5 Patcher

The following tools could be recognized as Patchers:

1. Patch-Engine[15]

2.6 Compressor

The following tools could be recognized as Compressors:

1. UPX [16]
2. ASPack [17]
3. PECompact [18]

2.7 Analyzer

The following tools could be recognized as Analyzers:

1. PEBrowse Professional [19]

2.8 Monitoring Tool

The following tools could be recognized as Monitoring Tools:

1. RegMon [20]
2. FileMon [21]
3. ListDLLs [22]

[9] https://www.hex-rays.com/products/ida/
[10] https://vetusware.com/download/windasm\%208.93/?id=12732
[11] https://docs.microsoft.com/en-us/dotnet/framework/tools/ildasm-exe-il-disassembler
[12] https://web.archive.org/web/20080214075546/http://www.kpdus.com/jad.html
[13] https://www.red-gate.com/products/dotnet-development/reflector/
[14] https://www.sothink.com/product/flashdecompiler/
[15] https://www.softpedia.com/get/Programming/Other-Programming-Files/Advanced-Patch-Engine.shtml
[16] https://upx.github.io/
[17] http://www.aspack.com/
[18] https://bitsum.com/portfolio/pecompact/
[19] https://download.cnet.com/PEBrowse-Professional-64-bit/3000-2218_4-75176627.html
[20] https://docs.microsoft.com/en-us/sysinternals/downloads/regmon
[21] https://docs.microsoft.com/en-us/sysinternals/downloads/filemon
[22] https://docs.microsoft.com/en-us/sysinternals/downloads/listdlls

4. PsList [23]

5. TCPView [24]

6. WinObj [25]

2.9 Protector

The following tools could be recognized as Monitoring Protectors:

1. armadillo [26]

2. obfuscator [27]

3 Conclusion

In this article, we reviewed the concept of Reverse Engineering along with a set of tools regarding that title.

References

[1] Wikipedia, "Reverse engineering." https://en.wikipedia.org/wiki/Reverse_engineering, September 2019. Accessed on 2020-1-30.

[2] anonymous007, "Software re-engineering." https://www.geeksforgeeks.org/software-re-engineering/, September 2019. Accessed on 2020-1-30.

[3] Wikipedia, "Hex editor." https://en.wikipedia.org/wiki/Hex_editor, September 2019. Accessed on 2020-1-30.

[4] Wikipedia, "Debugger." https://en.wikipedia.org/wiki/Debugger, September 2019. Accessed on 2020-1-30.

[5] Wikipedia, "Disassembler." https://en.wikipedia.org/wiki/Disassembler, September 2019. Accessed on 2020-1-30.

[6] Wikipedia, "Decompiler." https://en.wikipedia.org/wiki/Decompiler, September 2019. Accessed on 2020-1-30.

[7] Wikipedia, "Patch." https://en.wikipedia.org/wiki/Patch_(computing), September 2019. Accessed on 2020-1-30.

[8] Wikipedia, "File archiver." https://en.wikipedia.org/wiki/File_archiver, September 2019. Accessed on 2020-1-30.

[9] Wikipedia, "Analyzer." https://en.wikipedia.org/wiki/Static_program_analysis, September 2019. Accessed on 2020-1-30.

[10] Wikipedia, "Obfuscation (software)." https://en.wikipedia.org/wiki/Obfuscation_(software), September 2019. Accessed on 2020-1-30.

[23] https://docs.microsoft.com/en-us/sysinternals/downloads/pslist

[24] https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview

[25] https://docs.microsoft.com/en-us/sysinternals/downloads/winobj

[26] https://github.com/patrickfav/armadillo/blob/master/README.md

[27] https://obfuscator.io/