Reverse Engineering

Amedeo Cavallo

1 Introduction

Reverse engineering is a process that examines an existing product to determine detailed information and specifications in order to learn how it was made and how it works. For mechanical assemblies, this typically involves disassembly and then analyzing, measuring and documenting the parts. Reverse engineering is not limited to mechanical components or assemblies. Electronic components and computer programs (software), as well as biological, chemical and organic matter can be reverse engineered as well. [1]

The process of reverse engineering of software aims at restoring a higher-level representation (e.g. assembly code) of software in order to analyze its structure and behavior. Today, software is usually distributed in binary form which is, from an attacker's perspective, substantially harder to understand than source code. However, various techniques can be applied for analyzing binary code.

2 Introduction2

We expect you to prepare a document with this template. This document's scope is to provide students with a written alternative to learn about the topic of the ACT course. This document should report the **theoretical information** discussed during classes. You should write all the information and reference that can be useful to understand the topic. Moreover, you need to report a **walk-through** of one challenge on the same topic. Think about you before taking ACT class and what you knew back then. You explain to your older self the topic. Use class recording and slides as a guide for what is the minimum information that is needed. Make great use of examples and drawings. You can use drawings from slides or make new drawings. In the following section, you will find some examples that help you to keep a consistent style. Make a reference for every picture or listing in the text. Use this figure reference as an example Figure 1.

If you need a reference to a link please use footnotes[1]. If you are referencing to a paper or book you the bibliografy.[**?**] Use texttt when refering to register name or code in general like `EIP` or `call`

[1] `https://jinblack.it`

You can start from this example to build your report. Include in your final submission all the source code needed to perform any edit in the future including images source as well.

Figure 1: Img example

2.1 Example of code

Here you can fine an example of how to add some code. It is using the package minted with basic option enabled. You can write code in place:

```
1  import numpy as np
2
3  def incmatrix(genl1,genl2):
4      m = len(genl1)
5      n = len(genl2)
6      M = None #to become the incidence matrix
7      VT = np.zeros((n*m,1), int)  #dummy variable
8
9      #compute the bitwise xor matrix
10     M1 = bitxormatrix(genl1)
11     M2 = np.triu(bitxormatrix(genl2),1)
12 ...
```

You can reference to a line The important line is line 5.

You can use an external file and ave the code as listing.

The important line is line 3 of Listing 1.

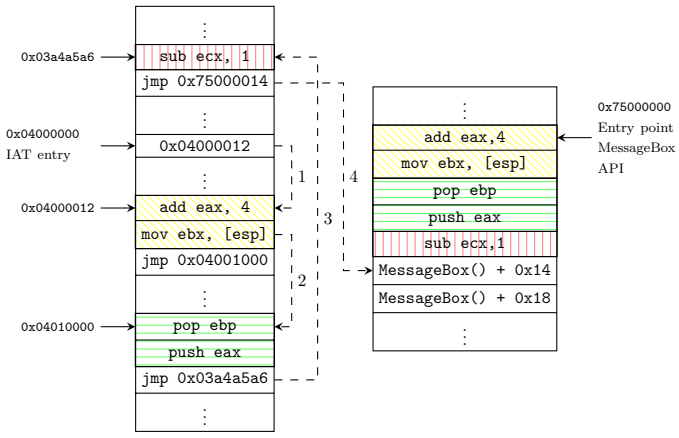

Figure 2: You can use tikz to draw nice memory drawing (example in file `stack_representation_example.pgf`.). Or google draw. If you use other tools, make sure to have all figure as `pdf`. Moreover, if you use an external tool, make sure to provide a way to modify the produced images. A link to google draw with correct permission is good enough.

3 Conclusion

"I always thought something was fundamentally wrong with the universe" [**?**]

References

[1] Ken Thayer. How does reverse engineering work? 2017.

```
import numpy as np

def incmatrix(genl1,genl2):
    m = len(genl1)
    n = len(genl2)
    M = None #to become the incidence matrix
    VT = np.zeros((n*m,1), int)  #dummy variable

    #compute the bitwise xor matrix
    M1 = bitxormatrix(genl1)
    M2 = np.triu(bitxormatrix(genl2),1)
```

Listing 1: Example from external file