International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Comprehensive Study of Current Reverse Engineering Tools and Techniques

Ohoud S. Al-Harthi[1], Emad S Al-Suwat[2]

Abstract: ***Reverse Engineering may be a mechanism concerned with discovering the technical principles of a machine or system by analyzing its structure, function and method of operation. Often this process is finished by analyzing a system (mechanical machine, software, electronic piece) into parts or trying to recycle the same system that performs the identical function because the original system. In other words, a rediscovery of the technical principles of applied mechanics through structural analysis processes, technological analysis, performance and performance analysis, and operating analysis, so the look data for a system or a product is reformulated to style new parts of the system so as to boost performance. This may be applied to mechanical installations, electronic components, software and others. Reverse engineering is also described as the physical measurement process of a part or a hand-made item, the production of an engineering form for it, the preparation of drawings manually or with the help of a computer, and the preparation of appropriate engineering data for recycling. An object is dismantled in detail to see how it works, and then a new device is redesigned that performs the same task. When using the software, a detailed analysis of the program is made with the aim of creating a new or improved program from the original program, without executing a duplicate of the program. An object is dismantled in detail to see how it works, and then a new device is redesigned that performs the same task. When using the software, a detailed analysis of the program is made with the aim of creating a new or improved program from the original program, without executing a duplicate of the program.***

Keywords: Reverse Engineering, Tools, Techniques

1. Introduction

The most traditional method used in technology development work is called advanced engineering. Technology workers develop their products using engineering and abstraction concepts. On the other hand, reverse engineering starts from the final product, and work is done back to reach the engineering concept by analyzing the required system, its partial components and analyzing the internal relationships of those partial components [1].

As for evaluation engineering, it is a designation that refers to an improvement process on a system or a product compared to the original product under analysis. There is an overlap in most cases between evaluation engineering and reverse engineering, because the goal of reverse engineering is also to make improvements and prepare documents that show how the original product works Detects hidden design. The performance of the product performed with reverse engineering efforts is very similar to the performance of the original product [2].

Reverse engineering has been applied throughout the ages to various economic activities, especially in industrial fields. Many countries have resorted to reverse engineering to study the products of other countries, and this industrial phenomenon escalated during and after the Second World War in all industrial fields, especially in the military fields.

Military forces have used reverse engineering most of the time to copy technology applied by another country, or to obtain information or models for weapons seized during combat, or by military intelligence, which was active in many times during World War II and during the Cold War.

The scope of work in the field of reverse engineering has expanded on information and communications technologies and on computers and equipment at the present time, as has also expanded in the fields of mechanical, electronic and chemical applications in all countries of the world to produce equipment and accessories or spare parts for equipment and machinery, or to convert unhelpful products into useful products By applying new technologies to old systems to adapt them to new information.

1) The motivations to use the reverse engineering

There are several reasons why we should conduct a reverse engineering process on a system:

- Interworking.
- Missing documents related to how a system was manufactured
- Analyze products to get an idea of how they work, especially in the case of historical devices and systems.
- Military or commercial espionage, knowing the plans and secrets of the enemy or the competing company.
- Copy protection breach.
- Create copies without a license or without the consent of the original owner.
- Academic education.
- Out of curiosity to know how things work.
- Learn from the mistakes of others, by making a better system than the first, after understanding how it works.

2) Reverse Engineering stages

Reverse engineering begins with defining the project goal, the appropriate method for determining the engineering shape of the required system and its parts, the appropriate accuracy of the cutting dimensions, and the method of using the results. This is done according to the following stages [3]:

The stage of determining the product (system or component of a system) that is subject to the reverse engineering process:

- One or several products are nominated for a reverse engineering project, and potential products for the project

Licensed Under Creative Commons Attribution CC BY

include individual materials, parts, components, units, and subgroups. Some of them may contain many small pieces. After studying the feasibility of the candidate products, one of them is determined for implementation of a reverse engineering project.

- The stage of analyzing the documented information and data on the way the original product works:
  This stage consumes the most time from the project implementation time, whereby the original product is dismantled into partial groups, then into its individual components, inventory of the raw materials used in the production of its components, specification of the chemical and physical specifications of the raw materials, and the approval of surface and thermal treatments for the different parts of the product, and determining the dimensions of Precision parts for preparing engineering drawings, designing peripheral tests, system performance tests and their partial components. After that, the basic specifications of the system are built with the help of technical data, and a working method is established for the system to be produced. Three-dimensional graphics are prepared using computer-aided design, through software for central computer systems, which helps to complete reverse engineering or make a modified design over the original design.
- The stage of using technical data and engineering plans generated by reverse engineering for a true copy or a modified copy of the original copy: At this stage, the engineers validate the data and plans resulting from the process of dismantling the product, then a careful reconstruction of the original system. The engineers also verify the validity and validity of the designs by testing the system, and then implementing a prototype for the new product, testing it, and documenting the test results. Where data and plans are checked and inspected for each stage with the help of computers, with the active participation of inspection and quality control services.
- The stage of implementing the new product and submitting it to the markets:

After successful implementation of the prototype, applying all peripheral tests, and performance tests, and ensuring the safety of product performance compared to the performance of the original model, the new product can be put on the market.
The new system is a competitive design in the market, as it depends on the creativity of the original product in terms of technical specifications, its efficiency and artistic age, with improvements to it, and the use of technologies that enable the new product to compete in terms of quality and financial value[4].

3) Reverse Engineering Applications

Reverse engineering is applied after reaching to understand the mechanism of work of any device or program, and to understand the mechanism that impedes the work of any device or program, and there are various applications of reverse engineering, including:

- Knowing and understanding a product, then developing it to work with better specifications than before.
- Study the design principles of a product as part of an educational process in the fields of applied sciences.
- Achieving compatibility between products and systems so that they can work together, or have common data as a result of the complexities of the products and the large number of parts, and this is included in the assembly of those systems and products; it is necessary to take into account when designing the parts of any product or exchange system and its production replacing the parts Among them the same product.

There is also a need to take into account the compatibility of the system or product with the attached products necessary for the system or product to perform the various tasks designed for it.

For example, the computer is compatible with the accessories required to perform the various functions needed and designed for it, such as the printer, laser scanner, "camera", connection with other computers, and the use of various software, among others.

- Quality control: to audit designs and products and correct errors in time:

Reverse engineering since 1992 performs great services to control quality, and experiences in this field have evolved and have become high-level, they have contributed to protecting customers and achieving the goals of different projects, determining the final engineering shape and measuring its dimensions and understanding the project needs are the first steps in reverse engineering.

ISO 17025 is used in conjunction with reverse engineering to control product quality, where computer inspection is carried out and by comparing the first piece of production on the production line with the designed model, and three-dimensional scanning is used in projects of reverse engineering and inspection of parts and generating surfaces to compare the product part of the original design to ensure From the integrity of the charts and documents, this is followed by another step to verify the quality with the help of computers and applied along the production line, and on operational operations to ensure full awareness of any engineering form, regardless of its complexity. Computer-aided design operations were applied to the manufacturer Manual and the required accuracy of any handcrafted was reached.

After the production of the handicraft and passing the two stages of inspection and verification with computer aided, the work is subjected to a final examination by an expert engineer before submitting the results and giving the order to continue the production.

From the foregoing it is concluded that the productive companies always focus on reverse engineering and dimensional inspection service to reach high quality products and accurate results, and to ensure the ability to maintain that over time, while producing successive batches of the product.

- Reverse engineering for computer programs:

Reverse engineering of a program means entering the program instructions and the possibility of modification therein, and these instructions are displayed in the assembly

Licensed Under Creative Commons Attribution CC BY

language, where the program of this language converts the text into the machine language regardless of the original language in which the original program is written.

Reverse engineering of binary software technologies can be accomplished in various ways, including: the way to dismantle programs, or to dismantle translation of the soft architecture of a computer program.

The process of dismantling the program means converting the original program itself from the assembly language to the machine language, as well as dismantling the translation, which means converting the original program text into the assembly language and then to the machine language.

- Producing an accurate digital model of any physical form:

The use of automated reverse engineering software is ideal for emergency and rapid applications such as the quantitative production of bespoke products, and for the reproduction of heritage products of high value.

The creation of algorithms to automate surface survey speeds up results, and improves the quality of surfaces for "models" and models produced on computer-aided or machine-assisted design. The use of computer technology in design and production leads to a tenfold increase in production rates compared to the use of traditional computer aided design software.
The use of automated measurement, design and production processes simplifies workflow, reduces training time and increases employee satisfaction due to the elimination of focused and tedious work tasks.

In the world today, companies specialize in completing prototypes for digital form, testing and processing, and for all types of industries and their applications.

4) Reverse engineering tools

The most important of them today are: computers, software, various measuring tools, chemical laboratories for the analysis of raw materials, laboratories for measuring the physical specifications of raw materials and programmed operating machines.
Today an integrated work system consisting of laser measuring machines with the help of special software is used to scan the dimensions of any piece and send it directly to computerized operating machines with numerical control and using computer aided design programs, and then creating a program for the programmed operating machine so that the machine can operate the piece and inspect it, and inspect the wear of tools Operating parts. As for the physical measurement process, it can be done using one of the following methods:

- Conventional linear measuring instruments for one dimension (special leveling tables pacolias (sliding measurement tools) - micrometers - precise markers).
- Optical projection for linear measurements of two dimensions.
- Fixed and portable three-dimensional contact measurement equipment.
- Computers to analyze geometric figures and special programs for analyzing two-dimensional and three-dimensional shapes.
- 3D laser measuring equipment.
- Equipment for measuring surface topography, roughness and straightness checks.

It is important that the correct method is chosen to overcome the dimensions of the engineering shape of the reverse engineering project. The choice of method depends on the complexity of the geometry of the part, the accuracy required for the product, the frequency of use of the measurement results, and the possibility of automatic reproduction of the engineering shape using the technical basis for design, measurement and computer-aided operation.The completion of this work requires high industrial, programmatic and inspection experience that must be enjoyed by engineers and technicians who will work in this field [5].

2. Software Reverse Engineering Tools

- **IDA Pro**

IDA Pro from Hex-Rays is the topmost reverse-engineering tool. It's an eccentric part of software.IDA Pro is an online disassembler, coded in C++, that runs on different operating systems.

- **Ghidra**

Ghidra is a reverse engineering framework for software that has been developed by the NSA for more than a decade. Essentially, the Reverse Software Engineering tool helps in detecting the source code of a special program that gives you the ability to detect potential virus threats or errors. Ghidra is a Java-based application available for Linux, Windows, and macOS[6].

- **Binary Ninja**

Binary Ninja finished by (Vector 35), it provides world-class analysis capabilities for security experts in the "PoliSwarm"ecosystem.It supports Ubuntu, macOS 10.13, and Windows 10 with 64-bit Linux, as well as PE. COFF, ELF, Mach-O, .NES, and Binary raw files.

- **Hopper**

Hopper is a disassembler for Linux and the macOS. It can disassemble, decompile, and debug executables 32-bit and 64-bit. Mac version uses Cocoa framework, while Qt 5 is included in the Linux edition. Hopper has an SDK that helps you to expand your functionality and even write your own software and CPU power. Additionally, certain functions of the program can be accessed from Python files, allowing you the ability to transform binaries.

- **Radare2**

The tool is used to perform reverse engineering. It allows you to perform reversing on programs, disks, a network, or even a system nucleus. It depends on the terminal interface. You can analyze, disassemble, and correct data, compare data, search, and replace. Itwas written in various languages such as Python, Ruby, JavaScript, Lua, and Perl.

Licensed Under Creative Commons Attribution CC BY

- **APK Tool**

The APKTool works by converting the dex files into smalifiles, and their context files are similar to a language called Jasmin. One of the most important features of the APKTool tool is that it has the ability to make decompile of the applications, and you can then modify them and re-create a recompile again to create a new apk file.

3. Conclusions

The implementation of reverse engineering technologies was very unhurried in industry. Reverse engineering is therefore done in order to retain the existing technology. Therefore, in its position it should not be based on software comprehension but on device survival. This may be exhausted by some technique which emancipates us from reverse engineering of a program over time due to changes prepared to its cipher. Scientists will go on to improve technologies plus methods used for basic inversecommercejobs, mainly for factsinversecommerce, however potential investigations will be vigilant to make the reverse engineering process more reproducible, Separate, controlled, and optimised. In broad changing environments, forward and reverse innovation processes must be merged and similar product and process enhancement tolerance in long-term growth as in the original production phases must be accomplished. It is impossible to foresee all the needs of the reverse engineers and therefore resources that are programmable for end-users must be created. Pervasive scripting is one effective technique for helping the user to codify, modify and automate ongoing considerate behaviors and to incorporate the reverse engineering software into the process and atmosphere of personal growth at the undistinguishable period. Device infrastructures Management has advanced melodramatically where power, data and visualization management technology is expected to continue to evolve at unprecedented levels. Whether we are perfecting reverse engineering technologies or not, the emerging legacy networks face inherent high costs and risks. Developing methods for managing these costs and risks may be a crucial path for long-term studies. The concept that reverse engineering must be continually implemented over the lifespan of the device, it is necessary to learn and theoretically recreate the earliest architecture and architectural decisions Implications on architecture. Reverse engineering needs to be cautious about recovery of the product. Because we want sophisticated tool support to effectively conduct device maintenance, official methods [7] have to be maintained to the recovered specification.

References

[1] R. K. Keller, R. Schauer, S. Robitaille, and P. Page, “Pattern-Based Reverse-Engineering of Design Components”, Proceedings of the International Conference on Software Engineering, Los Angeles, CA, USA, 1999, pp. 226-235.
[2] S. Masiero, “Design Pattern Detection in Reverse Engineering – The Role of Sub-Patterns”, Master Thesis, University of Milano-Bicocca, Milan, Italy, October, 2004.
[3] I. Philippow, D. Streitferdt, M. Riebisch, and S. Naumann, “An Approach for Reverse Engineering of Design Pattern”, Software and Systems Modeling, Springer Verlag, April 2004.
[4] S. R. Tilley., The Canonical Activities of Reverse Engineering. (Baltzer Science Publishers, The Netherlands. 2000.
[5] CHEN Hong-yuan ' LIU Dong. Key techniques and latest development in reverse engineering of objects[J]. JOURNAL OF MACHINE DESIGN, 2006, 23(8):1-5.
[6] WANG Qin-feng ' HU Zhi-chao ' ZHANG Huo-tu ' et al. Research and application on the reverse engineering design of automobile panel[J]. Machinery Design & Manufacture, 2011(4):83-85.
[7] MA Hanwei. Discussion on the Reverse Engineering Technology and Its Application in Industry[J]. Modern manufacture technology & ordnance, 2009(5):24-25.

Licensed Under Creative Commons Attribution CC BY