ASH1925009M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:06AM (UTC-0500)
Submission ID: 1782979807
File name: ASH1925009M.pdf (373.53K)
Word count: 1291
Character count: 7164

Reverse Engineering and Vulnerability Analysis

Abdullah Alif
ASH1925009M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security ....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

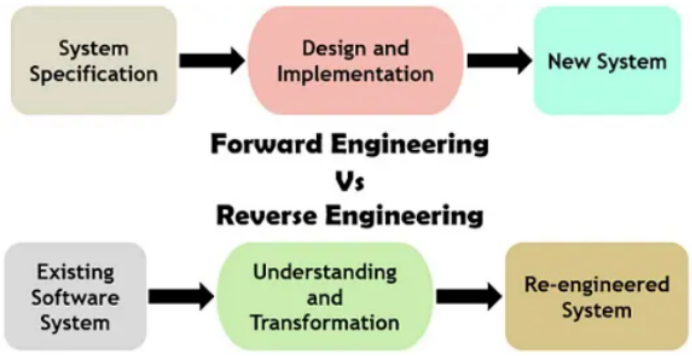
REVERSE ENGINEERING : The process of taking a piece of software or hardware and analyzing its functions and flow of information so that its function and behavior are understood.

This paper will be introduced with reverse engineering and vulnerability analysis.

1 Introduction

Reverse Engineering occurs when you take a finished product and work backward to determine how it was constructed or engineered. By breaking a product or piece of software down into its parts you can extract a good deal of information about the product. This strategy is very common in forensic investigations to determine the root cause of how a breach occurred. Reverse Engineering occurs when you take a finished product and work backward to determine how it was constructed or engineered. By breaking a product or piece of software down into its parts you can extract a good deal of information about the product. This strategy is very common in forensic investigations to determine the root cause of how a breach occurred. [2]

Figure 1: Reverse Engineering



The Purposes of reverse engineering:

1. used as learning tools
2. security auditing
3. enabling additional features
4. developing compatible products cheaper than that are currently available in the market

2 Background

Although many people believe that reverse engineering began in the 18th century with the introduction of the factory system, this is not the case. Reverse engineering has existed since the beginning when humans made things, such as wheels, carts, and even building infrastructure. To re-create these things, retrospective engineering was used — as irrational as it once was. The size of the object is taken, whole or in part, and rebuilt. For example, the Roman Army, which did not have a naval base until after the First Punic War, was able to recapture the Carthage quinquereme engineer in 264 BC. Thanks to the well-known Roman ingenuity, they built — and maintained a network of 300 ships in three months that were capable of surpassing Carthage vessels by numbers and sophisticated navigation systems. The retrospective engineering methods have changed significantly since then. Although backward engineering may begin with military programs, it is now useful in many different fields, including manufacturing. Over the years, many different technologies have been used by manufacturers to obtain object measurements and import them into CAD 3D modeling software. Integrated measuring machines (CMMs), test systems, and robotic arm-mounted talking devices have been used extensively in retrospective engineering to eliminate manual problems. Choosing to use one 3D measurement technology over another depends on the required tolerance levels, data density and speed, component features, line of sight, and ease of operation. Today, manufacturers are increasingly using portable 3D scanning engineering scanners. The reason? They produce very accurate, reliable, and repetitive results, such as the technology mentioned above. However, they are quick. It is also easy to use operators of any skill level and 3D component data can be found right at the bottom of the store.

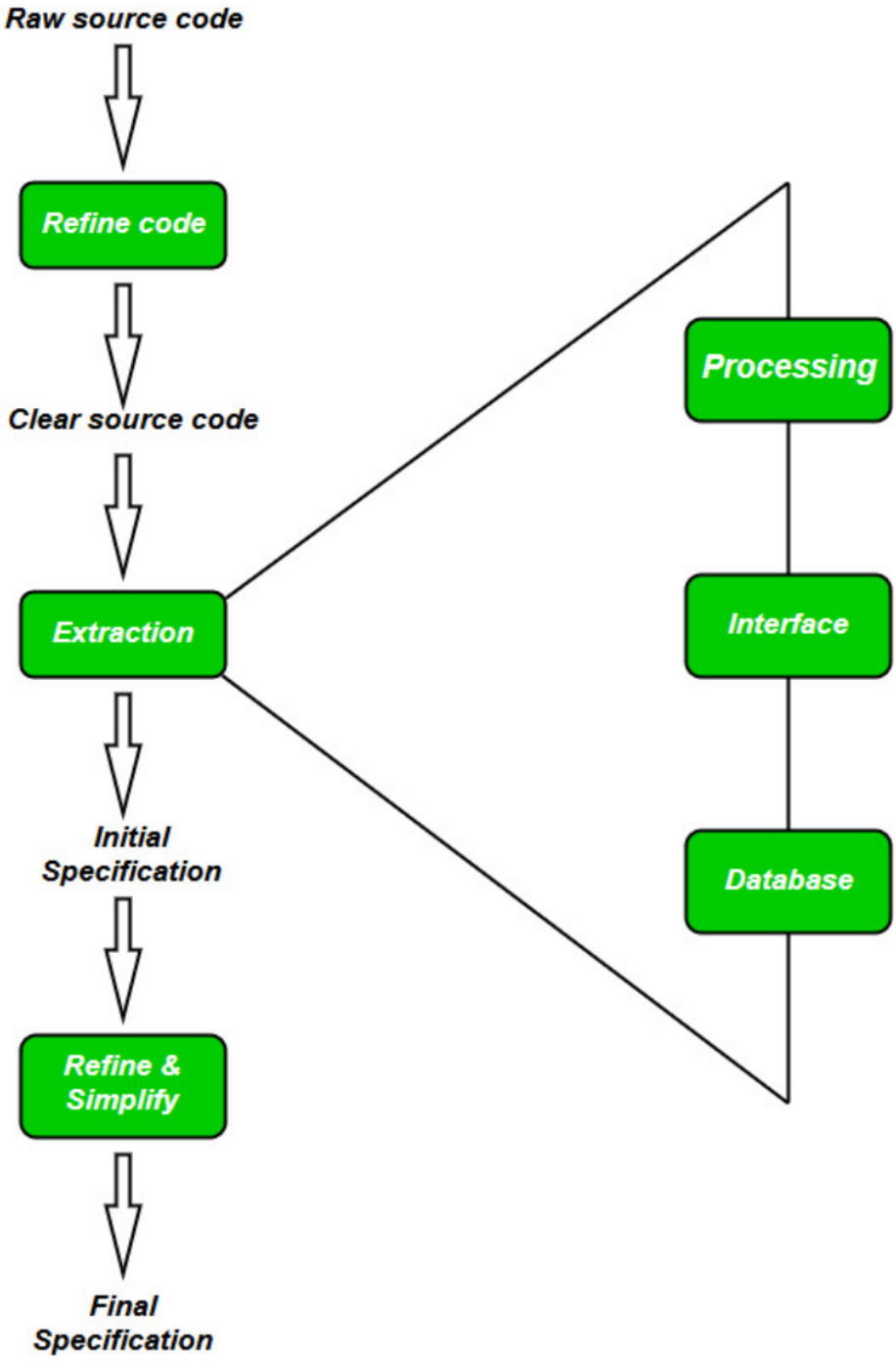
[1] [3]

3 Methods

Many UML tools refer to the process of importing and analyzing source code to produce UML drawings "as distorted engineering. Although UML is one way to provide "backward engineering" the most recent advances in international standards activities have led to the development of the Knowledge Discovery Metamodel (KDM). The standard brings an ontology of moderate (or abbreviated) representation of programming language and its relation. Object Management Group (on its way to becoming an ISO standard as well), KDM has begun to take the lead in the industry with the development of tools and analytical tools that can bring out source and analysis of source code, binary, and byte. Source code analysis, KDM architecture standards enable software system flow (data, control, and call maps), properties, and business layer information (rules, policies, and procedures). The standard allows the use of a standard data (XMI) format that allows for the integration of various levels of system information for detailed analysis (such as root cause, effect) or obtained analysis (such as extracting a business process). Although efforts to advocate for language development do not cease due to the number of languages, the continued development of software languages, and the development of new languages, the standard allows for the use of extensions to support a wider language set as well as evolution. KDM works with UML, BPMN, RDF, and other standards that allow for migration and thus utilizes system information through efforts such as software system modification and analysis of the business process layer.

[1]

Figure 2: Reverse Engineering process



4 Results

Interfacing. Reverse engineering can be used when a system is required to interface to another system and how both systems would negotiate is to be established. Such requirements typically exist for interoperability.

Military or commercial espionage: Learning about an enemy's or competitor's latest research by stealing or capturing a prototype and dismantling it may result in the development of a similar product or a better countermeasure against it.

Obsolescence. Integrated circuits are often designed on proprietary systems and built on production lines, which become obsolete in only a few years. When systems using those parts can no longer be maintained since the parts are no longer made, the only way to incorporate the functionality into new technology is to reverse-engineer the existing chip and then redesign it using newer tools by using the understanding gained as a guide. Another obsolescence-originated problem that can be solved by reverse engineering is the need to support (maintenance and supply for continuous operation) existing legacy devices that are no longer supported by their original equipment manufacturer. The problem is particularly critical in military operations.

Product security analysis. That examines how a product works by determining the specifications of its components and estimating costs and identifying potential patent infringement. Also part of product security analysis is acquiring sensitive data by disassembling and analyzing the design of a system component. Another intent may be to remove copy protection to circumvent access restrictions.

[4]

5 Conclusion

All software is coded. In fact, the code is what makes the whole system work the way it does. The code describes the software and the decisions it will make. Reversible engineering, as used in software, is a process of looking at patterns in this code. By identifying certain code patterns, the attacker could detect software vulnerabilities. [4]

References

[1] Eldad Eilam. Reversing, secrets of reverse engineering wiley publishing, 2005.

[2] M. G. Rekoff. On reverse engineering. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-15(2):244–252, 1985.

[3] Michael G Rekoff. On reverse engineering. *IEEE Transactions on systems, man, and cybernetics*, (2):244–252, 1985.

[4] Wikipedia. *Wikipedia*. PediaPress, 2004.

ASH1925009M

ORIGINALITY REPORT

61%	61%	1%	35%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	en.wikipedia.org Internet Source	29%
2	neometrixtech.com Internet Source	15%
3	arxiv.org Internet Source	6%
4	en.m.wikipedia.org Internet Source	4%
5	www.ukessays.com Internet Source	3%
6	global.oup.com Internet Source	3%
7	Submitted to Kaplan University Student Paper	2%
8	www.coursehero.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925009M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

PAGE 3

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

PAGE 4

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

PAGE 5

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

PAGE 6

PAGE 7

Possessive This word may be a plural noun and may not need an apostrophe.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 8

PAGE 9