Apr 3rd, 11:00 AM - 2:00 PM

Cognitive Understanding of Reverse Engineering Assistant

Nathan Elliot Harris
Cedarville University, nathaneharris@cedarville.edu

Bertrand L. LaChance
Cedarville University, blachance@cedarville.edu

Jeremy William Tiberg
Cedarville University, jeremywtiberg@cedarville.edu

Faith Trautmann
Cedarville University, ftrautmann@cedarville.edu

School of ENGINEERING and COMPUTER SCIENCE
CEDARVILLE UNIVERSITY

C.U.R.E. Assistant

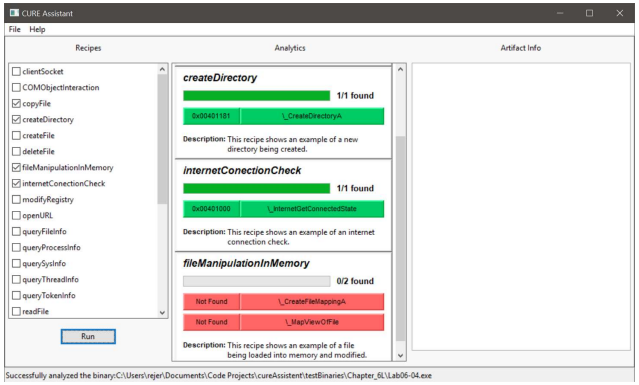
Reverse Engineering Educational Software

Faculty Advisor: *Professor Dudenhofer*
Students: *Bert LaChance, Faith Trautmann, Jeremy Tiberg, Nathan Harris*

Research & Scholarship SYMPOSIUM

Key Terms

- **Reverse Engineering:** Carefully examining and dissecting a product to figure out how it can be reproduced.
- **C.U.R.E.:** Stands for Cognitive Understanding of Reverse Engineering. The examination of the psychology and process of reverse engineering.
- **Disassembly**: The result of taking a binary and translating it into assembly instructions.
- **Assembly**: The lowest-level set of instructions that makes up a program above binary.
- **Binary**: The binary language is a 2-base number system used to represent all computer instructions. A binary is an executable file like a word processor, internet browser, etc.



How C.U.R.E. Assistant Works

The diagram on the bottom right demonstrates how C.U.R.E. Assistant works.

What are Recipes?

Recipes are "signatures" or chunks of code that perform a specific action or serve a specific purpose. C.U.R.E. Assistant uses a specific layout in JSON in order to search for these chunks of code. Experts can create recipes for different things they would normally look for, and supply them to the program. The novice would then take these recipes and use C.U.R.E Assistant in order to look for these things

What Happens When I Click "Run"?

After the user selects a binary to analyze, and the recipes they want to look for, C.U.R.E Assistant then goes through the following steps:

1. Loads in the recipes selected
2. Disassembles the binary provided using the program "Radare 2"
3. Uses pattern matching to analyze the binary and look for matches with the recipes that were loaded in
4. Stores the detected recipe information
5. Displays the results of the analysis to the user, where it found each part of the recipe, and a description of what that recipe means.

After C.U.R.E Assistant shows the results, the user can click on the addresses to copy a command for Radare 2 that takes them to the specific line of assembly

Abstract

The Cognitive Understanding of Reverse Engineering Assistant, or C.U.R.E. Assistant for short, is an independently developed program with the purpose of introducing students of the software reverse-engineering world to the art of disassembly. Reverse Engineering, or R.E. for short, is the process of deducing the source instructions or mechanisms of a device. This can be done to software to figure out how it works and how it can be exploited. While hackers employ this method for breaking into software systems, this is very useful for security researchers to determine security vulnerabilities in internet browsers, operating systems, apps, and more, so they can fix the problems before people using the software get exploited. Unfortunately, this is a very difficult and even expensive skill to learn, but C.U.R.E. Assistant seeks to mitigate that effort and cost. By analyzing a binary and then displaying the results in a user-friendly graphical-interface, C.U.R.E. Assistant is able to point out areas of interest to those who may not know what to look for or where to start. In addition, it is designed with added functionality to ease users into learning the intricate, but popular, reverse-engineering tool, Radare2. Inspired by the massive learning curve and scant available training for software dissection, C.U.R.E. Assistant aims to both streamline the process for experienced engineers as well as educate those new to the field in a friendly and informative manner.

Opinions on Reverse Engineering

The reverse engineering of software has many uses. It is helpful for understanding legacy software for which the source code has been lost. It can be used to analyze malware to see what negative effects it will have on a computer system. It is useful for finding hidden features in software or to simply satisfy curiosity about how a particular piece of software works. Reverse engineering can also be used for less innocent purposes. It can be used to steal software by breaking DRMs and for the unlawful duplication of software. Most commercial producers of software do not want their products to be reverse engineered because the way that the software works is considered to be a company secret. Doing this will usually violate the license and could potentially land the reverse engineer in legal trouble.