Fall 2021

Section 1: TTh 3:30pm - 4:45pm - JFSB B092 (changed from MARB 130)

Project 8: Extracting Secrets

Objectives

In this lab you will learn about the fundamental difficulties in restricting what users can do with the data on their computers. You will also:

- Learn how any traditional content restriction mechanism can be easily circumvented.
- Learn how "protected" data can be easily extracted from any application.

Overview

For many years, software companies have tried to restrict what users may do with the applications they buy. Often, these efforts have focused on preventing users from running applications on more than one computer. More recently, they've tried to restrict what users may do with data such as video, audio and even text.

In 1998, congress passed the Digital Millenium Copyright Act. Among other things, it specifies that "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." The problem with this clause as it relates to computers is that in their present state, no technological measures can effectively prevent a computer owner from accessing the data on his own machine!

Requirements

1. Download fortune_static, a statically linked Linux executable, and fortunes.enc, a file with encrypted content. When you run `fortune_static`, it will ask you for the "CD key," a password designed to restrict access to the program. You will not be given a valid CD key.
2. Use a debugger to bypass this password mechanism and make the program function normally. Instead of exiting, it will print out a random quote from the file `fortunes.enc`. This is done by modifying variables, registers, return addresses, etc. using the debugger. (See the ddd manual or gdb manual for help)
3. Now that you understand the code, open the executable in a hex editor (e.g., bless, vim) and modify the assembly code so that you can obtain a fortune every time you run the program. Perhaps any CD key that you enter will now work, for instance. You may be able to insert noops (0x90) to effectively crack the executable. Dr. Seamons was able to do this by modifying just one byte in the executable using vim as a hex editor. The result will be a new executable file that you can run and obtain a fortune.
4. Find a way to obtain all of the plaintext fortunes from fortunes.enc using the debugger.

Tips

To run `fortune_static` on a Linux machine, be sure it is set to be executable. You can do this with:

```
chmod u+x fortune_static
```

To disassemble `fortune_static` while keeping the hex values for each instruction that is executed, use the following command in the terminal:

```
objdump -d fortune_static > dump.txt
```

This will disassemble the entire program and store the result in the file dump.txt

Report

Generate a written report for the lab that addresses the following items. Please number each item for clarity.

1. How did you use the debugger to bypass the password mechanism? What variables did you modify? Please include a screenshot of the debugger in your report.
2. How did you edit the program to bypass the cdkey mechanism?

3. How did you obtain all the fortunes from the encrypted file?

Include the following in your report.

- a plain text section containing the list of all fortunes from the fortunes.enc file
- a screenshot of the debugger that shows you were able to access the plain text fortunes in memory.

NOTE:

- Using probabilistic methods to extract all the fortunes will not receive full credit. You should include a brief description of what you did to ensure that you have extracted all the fortunes. A NOT acceptable description would be "I ran the program 1000 times and collected all the unique outputs." An example of an acceptable solution would be "A used the debugger to change the output of the random number generator sequentially walking through all possibilities." or "I extracted the key that was used to encrypt the fortune file and decrypted it." or "I found where the decrypted fortunes were in memory and printed them all from there from the debugger." There are other possible methods of doing this which are likely acceptable.

Submission

Submit a PDF of your report on Learning Suite, including all the things asked for in each section.