ENEE459B: Reverse Engineering Lab
Homework #1

Overview

The ‘access’ executable provided in this HW is a piece of software used for granting access to a turnstile. It provides **simple user authentication** using standard username/password combinations. Unfortunately, the company that developed the software inserted **a backdoor to allow unfettered access** to all the organizations that use the physical access control system.[1]

Tasks

1. (**15 pts**) Find the routine that authenticates users (the main routine that finds the user and validates the password). What is **the address of the routine**?

2. (**20 pts**) Determine the **password encryption/obfuscation** method. **Add your own unique username and password** to ‘passwd’ and test that it works.

3. (**30 pts**) Decode the existing passwords in ‘passwd.’

4. (**35 pts**) Determine how the backdoor operates and how to use it. Explain all the steps.

[1] Crashing the process is not the backdoor because the physical system is engineered to fail secure (i.e., the door’s default behavior is to remain locked).