Indian Institute of Technology Palakkad
Department of Computer Science and Engineering
Operating Systems - Jul to Nov 2020
28 September 2020

Instructions:

- *Download the executable named 'vault'.*
- *If you manage to guess all the secret keys, or terminate by pressing CTRL+C, a log file will be generated. This log file will be named ROLLNO.log where ROLLNO is your roll number (example: 111801099.log)*
- ***Submit ONLY the log file on Moodle.***
- ***DO NOT EDIT/MODIFY THE GENERATED LOG FILE.***
- *This is an individual assignment. If you are taking help from your friends, acknowledge and give credit to them. Drop a mail informing the same.*

1. In this lab exercise, you are required to **guess three secret keys by analyzing an executable**.

   Assume the following scenario: You are working for a renowned spy/investigation agency (similar to MI6 from the James Bond series, or Sherlock Holmes). Your group is chasing a notorious criminal who has managed to steal some classified and highly sensitive documents, and has kept it inside his "next-gen" vault. Your field assistants have managed to break into his office, and copy the executable of the program that is managing the vault. Unfortunately they do not have the expertise to analyze the executable to guess the secret keys. It is your task to figure out the secret keys and pass it so that they can unlock the vault and recover the stolen documents. You have only one week to do this.

   CAUTION: You should use a combination of tools and commands such as `gdb`, `objdump`, `nm`, `strings`, `readelf`, etc. Be warned that you will be hopelessly lost **if you do not** take time (or breaks) to reflect upon the steps you are taking, search for alternative ways to achieve your sub-objectives, and strategize your next steps. There may be times where you will need patience and perseverance when solving this. Trying to solve it using brute-force may take too much time to solve this.