EN3240: Embedded Systems Engineering
Assignment 6 — Validation/Verification & Security

Name: Thalagala B. P.
Index No: 180631J

October 6, 2022

This is an individual assignment!
Due Date: 7 October 2022 by 11.59 PM

Instructions

Please read the instructions and questions carefully. Write your answers directly in the space provided. Compile the tex document and submit the resulting PDF. This is an individual assignment. You are not allowed to take or give any help in completing this assignment.

Problem 1 (1 Point)

How many input patterns (tests) are required (minimum) to verify a 3-input OR gate completely when only binary inputs are allowed (each input can be 0 or 1)? List the inputs and expected outputs.

Problem 2 (2 Points)

How many input patterns (tests) are required (minimum) to verify a 3-input OR gate completely when only ternary inputs are allowed (each input can be 0 or 1 or x; x implies unknown which can be 0 or 1)? List the inputs.

Problem 3 (2 Points)

There are two types of processor simulation techniques - functional and cycle-accurate. Given an input assembly program, the functional simulation produces the correct output but does not provide cycle-by-cycle details. On the other hand, the pipelined simulation provides a cycle-by-cycle simulation of the pipeline to eventually produce the final result. Which one is faster in terms of performance (simulation time) and why? Why do people use the slower one, then?

Problem 4 (2 Points)

There are only two ways of combining compression and encryption:

- CASE I: compression followed by encryption.
- CASE II: encryption followed by compression.

Please indicate which is beneficial for both code size reduction and security improvement. Please explain why the other one is not suitable.

Problem 5 (8 Points)

1. Download the shadow.hex file from the "assignment6-resources" folder. This file has been encrypted using RC4 encryption. 40 bits hexadecimal key: 6D 69 74 72 65. Decrypt the file using any available decryption tool (e.g., cryptool). Add a screenshot of the decrypted shadow.hex file content.

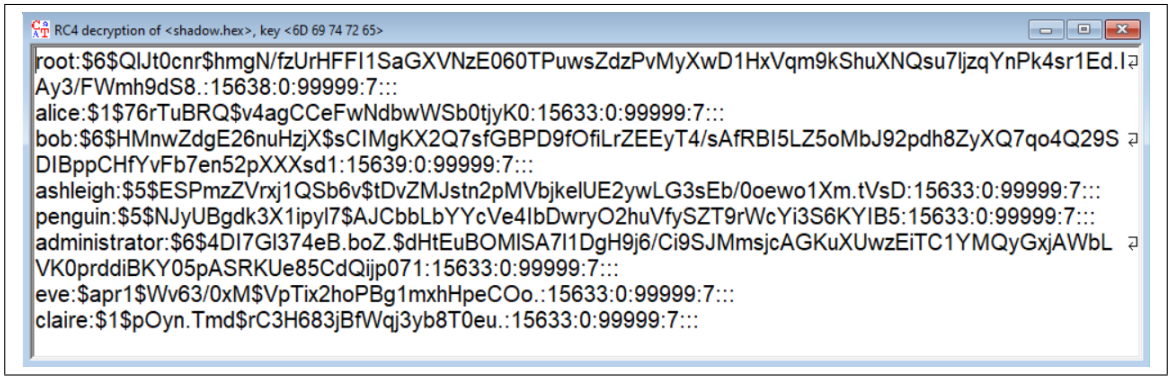

Figure 1: Content of the decrypted "`shadow.hex`" file

2. Run "John the Ripper" password cracking utility to crack the passwords in the decrypted shadow file with the help of the dictionary "rockyou.txt"(Link). What is the command you used to crack the passwords in the shadow file?

3. Add a screenshot of all the cracked passwords.

4. Provide recommendations to enhance the strength of the passwords.