CS 558 Introduction to Computer Security, Spring 2024

Written Homework Assignment 2

Total points 100

Out: 2024 Apr 15

Due: 2024 Apr 21 Sun. 23:59:59

Unnecessary long answers are usually from generative AI. Refer to the submission instructions for details of penalties.

1. (5 points each, prefer short accurate answers.) Recall the security related to software. Explain the following questions:

a. How is a canary used to prevent stack smashing attacks?
b. How can address space layout randomization prevent against buffer overflow attacks?
c. How the NX bit of stack can fight against buffer over flow attack?
d. Explain the difference between a virus and a worm.
e. Explain the difference between a polymorphic virus and metamorphic virus.

2. (5 points each, prefer short accurate answers) This problem deals with mandatory access control (MAC) and discre-tionary access control (DAC).
a. Define the terms mandatory access control and discretionary access control.
b. What are the significant differences between MAC and DAC?
c. Give one specific example where mandatory access control is used and give one example where discretionary access control is used.

3. (30 points)On a particular system, all passwords are 8 characters, there are 128 choices for each character, and there is a password file containing the hashes of 2^{10} passwords. Trudy has a dictionary of 2^{30} passwords, and the probability that a randomly selected password is in her dictionary is 1/4. Work is measured in terms of the number of hashes computed.
a. Suppose that Trudy wants to recover Alice's password. Using her dictionary, what is the expected work for Trudy to crack Alice's password, assuming the passwords are not salted? (List the equation to do the calculation is enough.)
b. Repeat part a, assuming the passwords are salted. (List the equation to do the calculation is enough.)
c. What is the probability that at least one of the passwords in the password file appears in Trudy's dictionary?(List the equation to do the calculation is enough.)

4. (30 points) Consider a government organization that uses a multi-level security (MLS) Bell-LaPadula (BLP) model with compartments to protect sensitive information. The organization has classified data into three levels: Unclassified, Secret, and Top Secret. Additionally, the data is compartmentalized into two separate compartments: Nuclear and Diplomatic.

John, a security analyst, has clearance at the Top Secret level and access to the Nuclear compartment. Mary, a foreign affairs advisor, has Secret level clearance with access to the Diplomatic compartment.

Given the scenario above, answer the following questions:

a. Can John access(read) information classified as Secret within the Nuclear compartment? Why or why not?
b. Can Mary access(read) information classified as Top Secret within the Diplomatic compartment? Justify your answer.
c. If a document is classified as Top Secret and spans both Nuclear and Diplomatic compartments, who can access(read) it?

Submission instructions

- Type your answers using whatever text editor you like, remember to include the index number of each question.
- Export the file to PDF format.
- Name the PDF file based on your BU email ID. For example, if your BU email is "abc@binghamton.edu", then the PDF file should be named as "hw2_abc.pdf".
- Submit the PDF file to Brightspace before the deadline.
- Do not copy/paste answers from generative AI(ChatGPT like tools). Once detected, you will get 0 out of 100 points. Unnecessary long answers have high chances copied from generative AI, and will be checked against tools.
- Do not copy other students work. Once detected, this behavior will be tread as plagiarism.
