Assignment 4

COMP 4290
Due: November 7, 2025 before 11:59 p.m.
Upload your Word, PDF, or zipped LaTeX file to Brightspace

Exercises from the Textbook (70 points):

Section 5.5: 9

Section 6.11: 4, 12, 14, 16, 22, 25, 27, 31, 42, 51

Section 7.7: 2, 5, 11

Additional Exercises (30 points):

1. Both Windows- and Unix-based systems primarily use a discretionary access control (DAC) model rather than a mandatory access control (MAC) model. Why do you think that is? Briefly describe a possible design for a MAC model for a consumer operating system and some of its challenges.

2. Similar to the example of the Bell-La Padula model discussed in the lecture notes, we will create a MAC system with four clearance levels, ordered from most secure to least secure: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), and UNCLASSIFIED (UC). We will also create categories of Batman, Robin, and Superman. Consider a user named Raúl who has a security level of {S, {Batman, Robin}}. Using precisely the same Simple Security Condition and *-Property as Bell-La Padula, state, for a file at each of the following security levels, whether Raúl has permission to read, to write, to do both, or to do neither.
    a. {C, {Superman}}}
    b. {TS, {Batman, Robin}}
    c. {S, {Batman, Robin}}
    d. {C, Ø}
    e. {UC, {Batman, Robin, Superman}}}

3. Firewalls can be used to defend against a SYN flood. Instead of allowing an outside client to send a SYN directly to a server, the firewall will remember the SYN and send a SYN/ACK to the client on behalf of the server. Then, when the final ACK comes from the client, the firewall will forward the original SYN to the server and then forward the ACK moments later. In this way, the server will not even begin a TCP connection until it has been completely established. What are the weaknesses of such a system? Is it possible for the firewall to be flooded so that it crashes?