ITIS 6200/8200 (Fall 2018)
Principles of Information Security & Privacy
Homework 4

Deadline: 11:59pm, November 30, 2018. No late submission will be accepted.
Submission method: upload your solutions to Canvas in a PDF file. The file name should be yourfirstname_yourlastname.pdf.
Each student is expected to finish this homework **independently**. NO COLLABORATION ALLOWED.
If you search the Internet, copy, and paste an answer, you will get zero.

1. A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.

a. Discuss how this technique might prevent legitimate users from accessing the system. Why is this action a violation of the principle of lease common mechanism?

b. One can argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state. Do you agree or disagree with this argument? Justify your answer.

2. Consider Multics procedures *p* and *q*. Procedure *p* is running and needs to invoke procedure *q*. Procedure *q*'s access bracket is (5, 8) and its call bracket is (8, 11). Assume that *q*'s access control list gives *p* full (read, write, append, and execute) rights to *q*. In which ring(s) must *p* execute for the following to happen? Justify your answer.

a. *p* can invoke *q*, but a ring-crossing fault occurs.
b. *p* can invoke *q* provided that a valid gate is used as an entry point.
c. *p* cannot invoke *q*.
d. *p* can invoke *q* without any ring-crossing fault occurring, but not necessarily through a valid gate.

3. A computer system provides protection using the Bell-LaPadula policy. How would a virus spread if
a. the virus were place on the system at system low (the compartment dominated by all other compartments)? Justify your answer.
b. the virus were place on the system at system high (the compartment that dominates all other compartments)? Justify your answer.

4. Classify the following vulnerabilities using the RISOS model. Assume that the classification is for the implementation level. Justify your answer.
a. The presence of the "wiz" command in the *sendmail* program (see section 20.2.8).
b. The failure to handle the **IFS** shell variable by *loadmodule* (see section 20.2.8).
c. The failure to select an Administrator password that was difficult to guess (see section 20.2.9).