Homework 4

Due: November 22, 2021 **Points:** 100

1. (*20 points*) A computer system provides protection using the Bell-LaPadula policy. How would a virus spread if:

   (a) the virus were placed on the system at system low (the compartment that all other compartments dominate)?

   (b) the virus were placed on the system at system high (the compartment that dominates all other compartments)?

2. (*25 points*) Assume that the Clark-Wilson model is implemented on a computer system. Could a computer virus that scrambled constrained data items be introduced into the system? Why or why not? Specifically, if not, identify the precise control that would prevent the virus from being introduced, and explain why it would prevent the virus from being introduced; if yes, identify the specific control or controls that would allow the virus to be introduced and explain why they fail to keep it out.

3. (*20 points*) In the Janus system, when the framework disallows a system call, the error code **EINTR** (interrupted system call) is returned.

   (a) When some programs have read or write system calls terminated with this error, they retry the calls. What problems might this create?

   (b) Why did the developers of Janus not devise a new error code (say, **EJAN**) to indicate an unauthorized system call?

4. (*25 points*) As encryption conceals the contents of network messages, the ability of intrusion detection systems to read those packets decreases. Some have speculated that *all* intrusion detection will become host-based once all network packets have been encrypted. Do you agree? Justify your answer. In particular, if you agree, explain why no information of value can be gleaned from the network; if you disagree, describe the information of interest and give an example of something network-based intrusion detection systems could detect but that host-based intrusion detection systems could not.

5. (*10 points*) Why is Spectre called a side channel attack rather than a covert channel?

Extra credit

1. (*20 points*) Euler's generalization of Fermat's Little Theorem says that, for integers a and n such that a and n are relatively prime, $a^{\phi(n)} \bmod n = 1$. Use this to show that deciphering of an enciphered message produces the original message with the RSA cryptosystem. Does enciphering of a deciphered message produce the original message also?