Homework #5

Due: June 2, 2021 **Points:** 100

Questions

1. (*24 points*) Consider Multics procedures p and q. Procedure p is executing and needs to invoke procedure q. Procedure q's access bracket is (5, 6) and its call bracket is (6, 9). 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?

   (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.

2. (*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)?

3. (*30 points*) Consider how a system with capabilities as its access control mechanism could deal with Trojan horses.

   (a) In general, do capabilities offer more or less protection against Trojan horses than do access control lists? Justify your answer in light of the theoretical equivalence of ACLs and C-Lists.

   (b) Consider now the inheritance properties of new processes. If the creator controls which capabilities the created process is given initially, how could the creator limit the damage that a Trojan horse could do?

   (c) Can capabilities protect against all Trojan horses? Either show that they can or describe a Trojan horse process that C-Lists cannot protect against.

4. (*26 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.