Homework 4

Due: November 25, 2019 at 11:59pm **Points:** 100

Questions

Remember to justify your answers.

1. (*10 points*) The second example in Section 16.2 asserts that UNIX file descriptors are in fact capabilities. Please explain in detail why this is true.
   Hint: How are file descriptors used?

2. (*20 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.

3. (*30 points*) Extend the semantics of the information flow security mechanism in Section 17.3.1 for records (structures).

4. (*20 points*) Consider the rule of transitive confinement. Suppose a process needs to execute a subprocess in such a way that the child can access exactly two files, one only for reading and one only for writing.
   (a) Could capabilities be used to implement this? If so, how?
   (b) Could access control lists implement this? If so, how?

5. (*20 points*) In the story " 'Repent, Harlequin!' said the Ticktockman" by Harlan Ellison, the Harlequin repeatedly disrupts schedules.
   (a) An "insider threat" is usually defined as someone who is trusted with access or information betraying that trust. It may be deliberate, the attacker knowing they are attacking; it may be unintentional, the attacker unaware of the effect of their actions. This story has a classic example of an unintentional insider attack. What is it? What might the consequences be? How does this relate to computer security?
   (b) Ellison uses an unusual style of writing in this story, in which he begins in the middle, then goes to the beginning, and then to the end. Further, the story has a manic quality due to the choice of words and its structure. How is this similar to handling a computer intrusion incident?

Extra Credit

E1. (*30 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?
   Hint: You must prove both the case where the message m and n are relatively prime, and where they are *not* relatively prime.