Homework 5

Due: June 7, 2018 at 11:59pm **Points:** 100

Questions

Remember to justify your answers.

1. (*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.

2. (*20 points*) Discuss controls that would prevent Dennis Ritchie's bacterium (see Section 23.6.1) from absorbing all system resources and causing a system crash.

3. (*40 points*) Classify each of the following vulnerabilities using the PA model. Assume that the classification is for the implementation level. Remember to justify your answers.

   (a) The presence of the "wiz" command in the *sendmail* program (see Section 24.2.9).

   (b) The failure to handle the **IFS** shell variable by *loadmodule* (see Section 24.2.9).

   (c) The failure to select an Administrator password that was difficult to guess (see Section 24.2.10).

   (d) The failure of the Burroughs system to detect offline changes to files (see Section 24.2.7).

4. (*10 points*) The C shell does not treat the **IFS** variable as a special variable. (That is, the C shell separates arguments to commands by white spaces; this behavior is built in and cannot be changed.) How might this affect the *loadmodule* exploitation?