Homework 1

Due: October 9, 2019 at 11:59pm **Points:** 130

Questions

Remember to justify your answers.

1. (*20 points*) How do laws protecting privacy impact the ability of system administrators to monitor systems for intrusions?
2. (*20 points*) The PostScript language describes page layout for printers. Among its features is the ability to request that the interpreter execute commands on the host system.
   (a) Describe a danger that this feature presents when the language interpreter is running with administrative or root privileges.
   (b) Explain how the principle of least privilege could be used to ameliorate this danger.
3. (*20 points*) Write a program that demonstrates when decreasing size between calls to `add_to_queue` causes elements previously added to the queue to become inaccessible. Describe the problems that can arise if the values of head and/or count are changed across calls to `put_on_queue`.
4. (*20 points*) A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.
5. (*20 points*) When you use an ATM at a bank, you receive a receipt that is, ostensibly, proof that the bank will accept as proof you withdrew the amount of money shown on the receipt. When you vote in the United States, you do not get a receipt enabling you to verify that your ballot was recorded and cast correctly. Give two reasons for this difference between the transaction with the bank and the transaction with the Department of Elections (or whatever the election office is called in your jurisdiction).
6. (*30 points*) In the story "Superiority" by Arthur C. Clarke, one mistake the narrator's military made was relying upon their superior science to defeat an enemy with vastly inferior science. In answering the following questions, show how your answer can be applied to, or says something about, computer security.
   (a) Prof. Norden's claims about the new weaponry were verified by experimentation. Yet the weapons failed to perform as they should have in battle. Why were the weapons so effective in Prof. Norden's experiments, yet such a failure when used in battle?
   (b) The Battle Analyzer was an automated system to analyze the enemy's positions and weapons used during a battle. It worked in one battle—the enemy was badly beaten—but not in the ones following that. What did the Battle Analyzer apparently fail to take into account?
   (c) What was the flaw in Prof. Norden's experiments testing the Exponential Field?

Extra Credit

E1. (*30 points*) Prove Theorem 4–1. Show all elements of your proof.