Homework 1

Due Date: April 13, 2011 **Points:** 100

Correction

In Problem 3, *add_to_queue* should be *put_on_queue*. I changed it here.

Questions

1. (*14 points*) Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination of each. Remember to justify your answers.
   (a) John copies Mary's homework.
   (b) Paul crashes Linda's system.
   (c) Carol changes the amount of Angelo's check from $100 to $1,000.
   (d) Gina forges Roger's signature on a deed.
   (e) Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
   (f) Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
   (g) Henry spoofs Julie's IP address to gain access to her computer.
   (*text*, §1.12, exercise 1).

2. (*10 points*) A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this?
   (*text*, §1.12, exercise 14).

3. (*36 points*) Write a program that demonstrates decreasing *size* between calls to *put_on_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*.
   ("Robust Programming" handout, exercise 3).

4. (*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.
   (*text*, §13.6, exercise 1).

5. (*20 points*) An attacker breaks into an IIS Web server running on a Windows 7-based system. Because of the ease with which he broke in, he concludes that Windows 7 is an operating system with very poor security features. Is his conclusion reasonable? Why or why not?
   (*text*, §23.9, exercise 6).

Extra Credit

1. (*15 points*) Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?