# Homework 1

**Due:** April 17, 2013 **Points:** 100

## Questions

Remember to justify your answers.

1. (*18 points*) Please characterize each of the following as one of snooping, masquerading, modifying, denying service, delaying, denying receipt, and repudiating origin.

   (a) Changing a love letter that your friend asked you to mail.
   (b) Writing a love letter and signing your friend's name.
   (c) Denying you wrote a love letter with your name signed.
   (d) Denying you received a love letter that your sweetie wrote you.
   (e) Not mailing a love letter that your friend gave you and asked you to mail.
   (f) Reading a love letter that your friend wrote.

2. (*12 points*) Please characterize each of the following as a component of a policy or as a mechanism.

   (a) You must be enrolled in an ECS class, or an ECS or CSE major, to have an account in the CSIF.
   (b) The systems staff (who administer the CSIF) check the enrollment lists that the registrar sends to the ECS department every night to determine who is enrolled in an ECS course.
   (c) Initial passwords are not to be posted downstairs because someone may copy them and use others' accounts without authorization.
   (d) The system staff runs the program *crack*, which guesses passwords, to determine if users have selected passwords that are too easy to guess.

3. (*20 points*) In Steve Bellovin's description of DRM [Bel07], he quotes Prof. Edsgar Dijkstra as saying "program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence."

   (a) Why is testing hopelessly inadequate for showing the absence of bugs? Please be detailed.
   (b) What point is Bellovin making by quoting this?

4. (*14 points*) In the `delete_queue` function in [Bis11], the `free` statement is not protected by an "if" that checks to see whether `queues[cur]` is **NULL**. Is this a bug? If not, why don't we need to make the check?

5. (*20 points*) An attacker breaks into a Web server running on a Windows 2000-based system. Because of the ease with which he broke in, he concludes that Windows 2000 is an operating system with very poor security features. Is his conclusion reasonable? Why or why not?

6. (*16 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.

## Extra Credit

7. (*20 points*) An organization makes each lead system administrator responsible for the security of the system he or she runs. However, the management determines what programs are to be on the system and how they are to be configured.

   (a) Describe the security problem(s) that this division of power would create.
   (b) How would you fix them?