Homework 4

Due Date: June 14, 2000, at 6PM **Points**: 150

1. (*50 points*) Consider the intrusion detection system model, which consists of sensor mechanisms, analysis engines, and notification engines. Please generalize this model to cover other system auditing mechanisms.
2. (*40 points*) The program *lsu* is a version of *su* that uses an access control file and the user's password to give access to shared accounts. It runs setuid to *root* on UNIX systems. On the web page is a tarball of the program *lsu.tar*. Download it and find at least 2 potential security vulnerabilities. You do ***not*** need to exploit them, but you must say how you could exploit them.
3. (*60 points*) The library *msystem* provides a version of the *system*(3) library function that purports to provide better security when invoked by a privileged (setuid or setgid) program. On the web page is a tarball of the library. Please evaluate it against the eight principles of secure design and state which ones it exemplifies, if any. Can you find any security flaws?