CS3235 Tutorial for week 13
(Nov 3rd-Nov 7th, 2003)

31st October 2003

1. **Question 2, Chapter 13 in textbook:** A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.

   (b) One can argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state. Do you agree or disagree with this argument? Justify your answer.

2. **Question 6, Chapter 13 in textbook:** Assume that processes on a system share no resources. Is it possible for one process to block another process' access to a resource? Why or why not? From your answer, argue that denial-of-service attacks are possible or impossible.

3. **Question 8, Chapter 13 in textbook:** A program called *lsu*[111] gives access to role accounts. The user's access rights are checked, and the user is required to enter her password. If access rules allow the change and the user's password is correct, *lsu* allows the change. Given that Mary uses *lsu* from her account, why does *lsu* require her to enter her password? Name the principles involved, and why they require this.

4. **Question 1, Chapter 14 in textbook:** (You should read section 14.6.2 in the textbook) The web site www.widget.com requires users to supply a user name and a password. This information is encoded into a cookie and sent back to the browser. Whenever the user connects to the Web server, the cookie is sent. This means that the user need only supply a password at the beginning of the session. Whenever the server requests reauthentication, the client simply sends the cookie. The name of the cookie is *identif*.

   (a) Assume that the password is kept in the clear in the cookie. What should the settings of the *secure* and *expires* fields be, and why?

   (b) Assume that the name and password are hashed, and that the hash is stored in the cookie. What information must the server store to determine the user name associated with the cookie?

   (c) Is the cookie storing state or acting as an authentication token, or both? Justify your answer.