Outline for November 24, 2003

Reading: Chapter 22.3–22.5

Discussion Problem

The program *sendmail* is a message transport agent; that is, it moves mail from one host to another. It also logs each use in the *syslog* file. One day, I observed the following entries:

```
Oct 28 06:14:15 nob sendmail[18680]: GAA18680: /bin/sed... Cannot mail
      directly to files
Oct 28 06:14:52 nob sendmail[18682]: GAA18681: to=<decode>,
      from=</dev/null>, delay=00:00:44, mailer=prog, stat=Sent
```

1. What is suspicious about the first *syslog* entry? What do you think the author of the first mail message was trying to do? Did it work?
2. The *decode* address passes a message to the *uudecode*(1) program. This program transforms the letter into a file, and puts it into the file system where the mail message says. What does the second message indicate?
3. What fundamental problem underlies both of these mail messages?

Outline for the Day

1. Malicious logic
   a. Quickly review Trojan horses, viruses, bacteria; include animal and Thompson's compiler trick
   b. Logic Bombs, Worms (Schoch and Hupp)