Homework 4

Due: Friday, March 7, 1997 at 11:59PM (note old time!)

Analytical

These are worth 40 points each.

1. Does the system of all subsets of a finite set, under the operation "subset of" ($\subseteq$), form a lattice? Either show that it meets all the requirements of a lattice, or state which requirement it fails to meet and prove that it fails to meet the requirement.
2. The UNIX operating system and its attendant programs assume that any incoming message with source port 1023 or less (the "privileged ports") was sent by a process running as *root*. Assuming the remote host is a UNIX system, is there any way that a process can send a network message from a privileged port when that process is not running as *root*?
3. IIn the ISO model, peer processes communicate without regard for precise implementation of activities at other layers. For example, the application does not know or care what specific routing has been chosen by the network layer. What is the security effect of an application program's not knowing the routing selected for a particular message, or even a particular session?
4. Where (at what times during its transmission) is a message exposed if it is protected by link encryption? Where is a message exposed if end-to-end encryption is used?
5. Is encryption an effective control against passive wiretapping? Why or why not? Against active wiretapping? Why or why not?

Programming

There is no program on this assignment. Please use the time for your projects, which are due on March 14!