Homework 4

Due Date: March 1, 2011 **Points:** 100

Questions

1. (*15 points*) Let $L = (S_L, \leq_L)$ be a lattice. Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice, where:
   (a) $S_{IL} = \{[a,b] | a,b \in S \wedge a \leq_L b\}$
   (b) $\leq_{IL} = \{([a_1,b_1],[a_2,b_2]) | a_1 \leq_L a_2 \wedge b_1 \leq_L b_2\}$
   (c) $lub_{IL}([a_1,b_1],[a_2,b_2]) = (lub_L(a_1,a_2), lub_L(b_1,b_2))$
   (d) $glb_{IL}([a_1,b_1],[a_2,b_2]) = (glb_L(a_1,a_2), glb_L(b_1,b_2))$

   (*text*, problem 16.2)

2. (*15 points*) Why can we omit the requirement $lub(\underline{i}, \underline{b[i]}) \leq \underline{a[i]}$ from the requirewments for secure information flow in the example for iterative statements (see Section 16.3.2.4)? (*text*, problem 16.5)

3. (*20 points*) Consider the rule of transitive confinement. Suppose a process needs to execute a subprocess in such a way that the child can access exactly two files, one only for reading and one only for writing.
   (a) Could capabilities be used to implement this? If so, how?
   (b) Could access control lists be used to implement this? If so, how?

   (*text*, problem 17.3)

4. (*25 points*) In the Janus system, when the framework disallows a system call, the error code **EINTR** (interrupted system call) is returned.
   (a) When some programs have read or write system calls terminated with this error, they retry the calls. What problems might this create?
   (b) Why did the developers of Janus not devise a new error code (say, **EJAN**) to indicate an unauthorized system call?

   (*text*, problem 17.5)

5. (*25 points*) In the covert flow tree technique, it is possible for some part of the tree to enter a loop in which recognition of attribute a depends on recognition of attribute b, which in turn is possible when attribute a is recognized.
   (a) Give a specific example of such a loop.
   (b) Should such a loop occur, the overt flow tree path is labeled with a *repeat* parameter that dictates the maximum number of times that branch may be traversed. Discuss the advantages and drawbacks of this solution.

   (*text*, problem 17.7)

Extra Credit

1. (*15 points*) Section 17.3.2.3 derives a formula for $I(A;X)$. Prove that this formula is a maximum with respect to p when $p = \frac{M}{Mm+1}$, with M and m as defined in that section. (*text*, problem 17.8)