Homework 4

Due Date: March 16, 2009 **Points:** 100

Questions

1. (*25 points*) In the flow certification requirements for the *goto* statement in Section 16.3.2.5, the set of blocks along an execution path from b_i to IFD(b_i) excludes these endpoints. Why are they excluded? (*text*, problem 16.6)

2. (*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)

3. (*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)

4. (*25 points*) Consider the RSH attack discussed in Lecture A-2 and [TL00]. An attacker uses that attack to alter a ".rhosts" file, enabling her to log in as a normal user. (Call this Exploit #1.) She then exploits a buffer overflow in a line printer daemon program (*lpd*) to acquire *daemon* privileges. (This is Exploit #2.) Finally, she uses her newly-acquired *daemon* privileges to exploit a race condition in a mail delivery program (*delivermail*) to obtain *root* access. (This is Exploit #3.)

   Please state the *minimum* set of capabilities that each exploit requires, and that each successful exploit provides. You may state the subjects, objects, actions, and other components of the capability informally—but be clear. Show how the provided capabilities and required capabilities match up.

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)