Homework 3

Due Date : March 2, 1999 **Points** : 200

1. (*20 points*) A computer security expert claims that one of the measures necessary to obtain computer security is the separation of programmers and operators Is she right? Justify your answer.
2. (*20 points*) Consider the UNIX file system.
   a. How could a mandatory access policy be defined so that a user has access to a file only if the user has access to all subdirectories higher (closer to the root) in the file structure?
   b. What would be the effect of this policy?
3. (*20 points*) Why is labelling (associating labels with objects and subjects) a security requirement? That is, why could a trusted computing base not simply maintain an access control table with entries for each subject and each object rather than having labels associated with each object?
4. (*30 points*)Compare the Clark-Wilson model rules to typical software engineering approaches for protecting abstract data types from program routines.
5. (*40 points*) Suppose information is classified on the basis of (i) content level (*C* for confidential and *S* for secret), and (ii) department (D_1, ..., D_4), where the relationship among departments is given by:

   $$D_1 \subset D_3 \subset D_4$$
   $$D_2 \subset D_4$$
   $$D_1 \cap D_2 = \varnothing$$
   $$D_2 \cap D_3 \neq \varnothing$$

   In case of proper containment, $D_i \subset D_j$, two distinct departments are assumed, D_i and $Dj–D_i$. If $D_i \cap Dj \neq \varnothing$ and there is no containment of one in the other, it is useful to define an additional department in the intersection. By the Bell-LaPadula Model, the natural permissible information flows are dictated by the partial orders (i) $C \subseteq S$ and (ii) $D_i \leq Dj$ if and only if $D_i \subseteq Dj$.

   Assume the set of security classes

   $$K = \{ (x, y) \mid x \in \{C, S\} \text{ and } y = \text{some department} \}$$

   Construct a lattice of secure information flow such that
   a. *K* contains a minimum number of classes; and
   b. $(x_1, y_1) \leq (x_2, y_2)$ if and only if $x_1 \leq x_2$ and $y_1 \subseteq y_2$.
6. (*70 points*) We are now going to test *lassen* from the point of view of the ordinary user. The goal is to perform any of the following: read the file /README, alter the file /CHANGEME, or lock up the system (a denial of service attack). As in the first homework, the first step in a penetration test is to hypothesize flaws, or potential vulnerabilities. For this exercise, you must assume you are analyzing the system as though you have no access to it other than from the network. You will hypothesize potential flaws and test them.
   a. Please devise three possible system-based vulnerabilities on the system. You are also to describe how to test for the flaw, possibly with the aid of an atack tool (but without one is fine, and indeed preferable). Your description should have the format given on the web page
      http://seclab.cs.ucdavis.edu/projects/vulnerabilities/doves/template.html
   b. Run your test and report the results.

   Please post your description, and the results of your attack, to the newsgroup *ucd.class.ecs253.d*.***Do not post any attack tools you use*** but do submit them with your answer to this question. Your submitted answer may be a copy of your news posting, plus any attack tools used. As part of the requirement for this answer, *each student must submit 3 different potential vulnerabilities*; the first poster of each vulnerability gets credit for it. So be sure your vulnerabilities are different than your classmates'!

   Each registered student in the class has been given an account on *lassen*. Your account name is the same as your name on *toadflax* or, if you do not have one there, on the CSIF. Your password is the first 8 digits of your student identification number as given by the registrar. ***Please change your password as soon as you log in*** .

Extra Credit

7. What assumptions with respect to trust would an implementation of the Clark-Wilson model make? In particular,

if you wanted to attack a system that implemented the Clark-Wilson model, what flaws would you hypothesize? Please discuss flaws related to the implementation and operation of system aspects related to the model *only* (that is, passwords being stored in the clear is not a relevant flaw).