CS181S – Systems Security Fall 2020

Problem Session 11: Mandatory Access Control (MAC)

Wednesday, November 11, 2020

1. **Multi-Level Security.** Consider a new scheme for implementing MLS confidentiality, where labels on files and programs can be changed according to the following rules.

   - At any time, the label $L(F)$ on a file F (i) can be increased or (ii) can be decreased to the largest label on any item that has been written so far to that file.
   - At any time, the label $L(Pgm)$ on any program Pgm (i) can be increased or (ii) can be decreased to the largest label on any item that has been read so far by that program.

   Moreover, assume that

   - If $L(Pgm) > L(F)$ then a write to file F by program Pgm—that is, a "write-down—is implemented as a "no-op (but does not cause program execution to be blocked or terminated).
   - If $L(Pgm) < L(F)$ then a read to file F by program Pgm—that is, a "read-up—returns "file unavail as if that is the contents of the file.

   Is there an environment where it is possible for a program Pgm to learn whether the contents of a file F satisfy some given predicate, even though $L(Pgm) < L(F)$ holds at the time the predicate is evaluated? (We define environment to mean: some set of files and other executing programs.) If so, describe the environment and the attack; if not, give an argument that explains why the information cannot be learned by Pgm.

2. **Information Flow.** Consider the following example programs. Which of these would you consider to satisfy noninterference?

   (a) P_1 executes the following code:

   ```
   while(H_in > 5){
       nop;
   }
   L_out = 4;
   return L_out;
   ```

   (b) P_2 outputs $L_{out} = H_{in} \oplus k$, where k is a freshly generated, uniformly random 32-bit value. Assume that H_{in} is always a 32-bit value.

   (c) P_3 outputs $L_{out} = \texttt{Enc}(H_{in}; L_{in})$. Assume that L_{in} is always a valid RSA key and Enc is RSA encryption.

   (d) P_4 takes a list of ballots as H_{in} and returns L_{out}, where L_{out} is the results of the election

   (e) P_5 takes a list of Pomona students $L_{in,1}$ and a list of dorm rooms $L_{in,2}$ and returns a list of room assignments L_{out}.