CS6600 Homework 6

Matthew Whitesides

I. CHAPTER 6 PROBLEMS

2) Under the low watermark policy, a subject lowers their integrity level to the level of the object being read or modified. An example is if integrity levels were mapped to Top-Secret (TS) and Secrete (S). Subject A who is at a TS level reads from an S level document. Their integrity level would drop to S. However, if subject A is reading from a TS (an equal level to themselves) level document, their level would be unchanged.

4) Essentially, the run-untrusted command delegates the actual function of executing a lower level program to another program; therefore, you do not have to lower your integrity level to run it directly. In theory, this program would have to reduce its level to run, meaning it would be exempt from the rule, so technically not any more or less secure. However, in practice, I think the extra step of the subject acknowledging that they're running a lower level program than themselves and it's untrusted is an extra step that ensures the subject knows the effects of running it.

9) In the Clark-Wilson model transformation procedures (TPs) are used to change the state of data from one valid state to another. These procedures must be executed in serial transactions as each change to state must be validated to be secure after every TP. If multiple TPs were executed in parallel it would be impossible to verify the validity of the final state and if not all transactions would have to be rolled back instead of the latest one.

11) ER1 establishes that a TP specifically can execute an object, and ER2 focuses that a user has rights to execute a TP, which in turn can execute an object. No TP can be executed without a subject doing so so you could combine the rights; however you wouldn't then be able to apply specific rights of a TP regardless of the subject executing it, one TP may have a set of an object that doesn't map directly to the objects a subject has, plus this is the whole point of having the TP to separate the user and the security of the TP executing the change of the object.

12) The Biba model enforces the following rules, and we will see how the Clear-Wilson model meets these requirements.

   a) S can read O if the integrity level of S is less than or equal to that of O's. This is achieved in CR2 that a subject is a subset of a CDIset, which is essentially an integrity level within that of O's.

   b) S can write to O if the integrity level of O is less than or equal to that of S's. This is established in CR4 in that TPs can append information (inherently at their level) and CR5 that only valid transformations ensuring that no user can create a TP that is higher than their level and only those TPs can execute on O.

   c) S1 can execute S2 in set S if the integrity level of S1 is less than or equal to that of S2's. This is mapped to the idea that subjects execute TPs at their level so two subjects could execute the same TP if both subjects were of an appropriate level, but no subject could execute a TP at a higher level.

ACKNOWLEDGMENT

Matthew Whitesides Master's Student at Missouri University of Science and Technology.