

# CS6600 Homework 3

Matthew Whitesides

## I. CHAPTER 3 PROBLEMS

- 1)  $A[s_1, o_1]$  and  $A[s_1, o_2] = A[s_1, o_2] \cup A[s_2, o_2]$  essentially says that the first two subjects created are able to give the entire scope of rights available to the system as not other subjects with lesser rights would be able to be created after that. This works because whatever initial rights  $s_1$  had over  $o_2$  would give the rights of any object not explicitly created for that object, plus the rights of a subject ( $s_2$ ) has over that object. If one could test for the absence of rights this statement would still be true however you wouldn't need to use both objects you could just do something like  $A[s_1, o_1] \cup (\forall r \notin A[s_1, o_1])$  just check for all rights and rights not in that to get the entire scope but that would be more operations.
- 2) We can omit the delete and destroy commands because they inherently cannot "add" rights they can only take them away. Therefore no leak could occur from those commands only the opposite of a leak which may not be optimal for a user but is secure. This would be different if we could test for the absence of a right however, given that we could use the test for absence to determine if a right has been deleted from a subject making the minimal set of operations reduced given we currently have to check each right.
- 3) a) Modifying the definition to say leaks occur beyond the initial state of the cell, then the delete and destroy commands would affect the ability to leak a right. If so we cannot get rid of them because we now have a definition where you can delete rights potentially all of a subject's rights, then any addition of any basic right would cause a leak.
- 4) First
- 5) First

## ACKNOWLEDGMENT

The author would like to thank Professor Bruce McMillin with the Department of Computer Science, Missouri University of Science and Technology.