Daniel Garcia

ECE 548

Homework 5

4.5 UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an **inode**. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?

**Answer:**

In the Unix filesystem, directory permissions are very important. Since members of the group can access the directory and can modify the directory, even though they cannot list the directory, it means that if a member of the group knows the name of the file, that person can also remove it because removing a file requires permission to write to the directory. The file permissions in this case do not really matter because the directory grants the owner and group enough access to the file that the file can be compromised.

In addition, a member of the owners group can remove the file if they know the name. They can also read the file if they know its name. These two facts make it very clear that the file is not being protected by the 644 ACL the way it was intended to be

4.9 The NIST RBAC standard defines a limited role hierarchy as one in which a role may have one or more immediate ascendants but is restricted to a single immediate descendant. What inheritance relationships in Figure 4.10 (Simple ABAC Scenario) are prohibited by the NIST standard for a limited role hierarchy?

**Answer**

Since the NIST hierarchy defines having only one descendant explicitly, that means the in the graph shown on page 132, directory and the project lead 1 & 2 roles, are invalid. This is they have more than one descendant. In order to restructure the graph to abide by NIST, the biggest change would be to put the production engineer and the quality engineers on different levels in the hierarchy, which would challenge those in charge of the hierarchy to decide which privileges are needed. If the same privileges are needed for both jobs, then a more generic name should be given to the same role to prevent the RBAC from snowballing and creating a laundry list of permissions many of which are duplicates of others.