

7

responsive to receiving a request from a user to run a command, determining if the user is assigned an accessauth for the command;

responsive to determining that the user is assigned an accessauth for the command, determining if a sub-command is a privileged sub-command, and responsive to determining that the sub-command is a privileged sub-command, accessing the command table;

responsive to accessing the command table, determining if the accessauth of the sub-command is included in an authorized authorization set of the command; and

when the accessauth of the sub-command is included in the authorized authorization set of the command, running the privileged sub-command;

whereby a privileged sub-command is run only when the command is run and cannot be run by the user in any other context or at any other time.

3. A non-transitory computer program product for causing a computer to provide an access control comprising:

a computer readable storage medium;

a program stored in the computer readable storage medium;

wherein the computer readable storage medium, so configured by the program, causes a computer to perform the following series of steps:

modifying an operating system to access a command table and to only run a sub-command when an appropriate authorization is in the command table;

8

modifying the role based access control system to eliminate inherited privileges;

entering a plurality of authorized access sets into the command table, the plurality of authorized authorization sets comprising a set of authorizations, each authorization corresponding to a privileged sub-command within a command;

responsive to receiving a request from a user to run a command, determining if the user is assigned an accessauth for the command;

responsive to determining that the user is assigned an accessauth for the command, determining if a sub-command is a privileged sub-command, and responsive to determining that the sub-command is a privileged sub-command, accessing the command table;

responsive to accessing the command table, determining if the accessauth of the sub-command is included in an authorized authorization set of the command; and

when the accessauth of the sub-command is included in the authorized authorization set of the command, running the privileged sub-command;

whereby a privileged sub-command is run only when the command is run and cannot be run by the user in any other context or at any other time.

* * * * *