RegalaFicheros.c

Resumen en lo que afecta a Credenciales

Tanto el user origen como el user destino son dos cuentas diferentes de unix, y cada uno tiene permisos rwx- - - - - - (700) con lo que solo pueden leer y escribir sus propios ficheros

El user origen es el propietario de RegalaFicheros.out (ejecutable) y le pone el setuid bit a 1 (rwsr-xr-x, chmod 04755 RegalaFicheros.out). Lo deja en /tmp (ahí todos tienen acceso para leer y ejecutar ficheros) o en un directorio donde el user destino tenga permisos de lectura y ejecución.

el user destino al invocar este ejecutable que tiene owner user origen y bit setuid=1, la llamada exec() hace que las credenciales para el proceso que ejecuta RegalaFicheros.out se cambien a
effective uid <-- uid user origen
saved uid <-- uid user origen
mientras que real uid sigue la del user destino que es la del proceso que ejecuta RegalaFicheros.out

De esta manera pueden leer los ficheros del user origen ya que para el acceso lo que rige es la effective uid.

Después de leer un fichero para poder escribirlo en user destino tiene que hacer setuid (user destino), de esa manera hace
effective userid <-- real uid (que es la de user destino) y que es operación permitida
y de esa manera puede escribir en user destino

para volver a leer en user origen tiene que hacer setuid (user origen)
y de esa forma hace
effective userid <-- saved uid (que es la de user origen) y que es operación permitida

y así sucesivamente

Las operaciones de read y write solo miran el fd para ver los permisos de read/write, las credenciales se miran en open (tienen que estar puestas en ese momento).