

# Seguridad y Algo I

Laboratorio de TOCTOU

Lic. Leandro Meiners



DEPARTAMENTO  
DE COMPUTACION

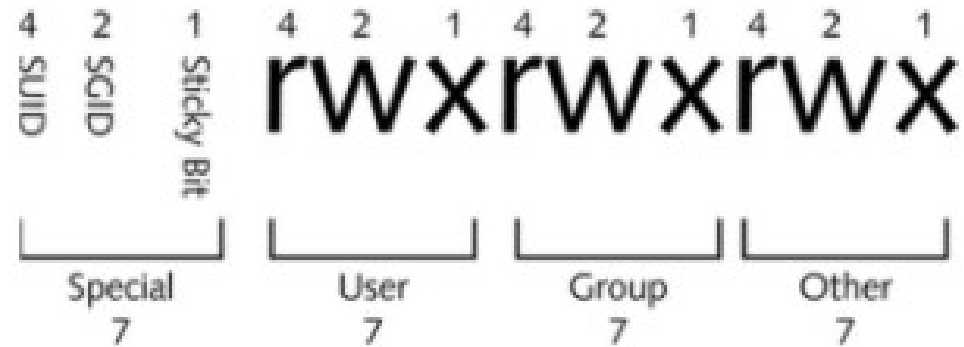
Facultad de Ciencias Exactas y Naturales - UBA

# Agenda

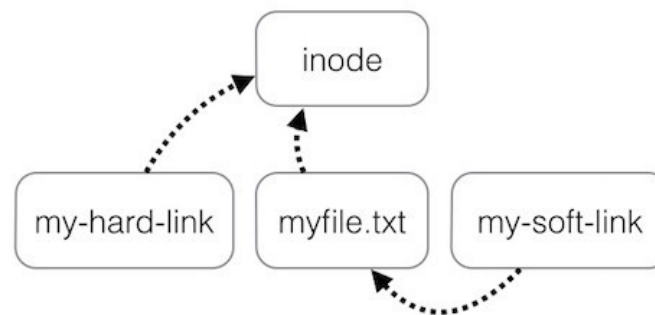
- Repaso TOCTOU
- Presentación del Ejercicio



# Permisos en Unix



## Links en Unix



# Ejemplo de Explotación mediante Symlinks

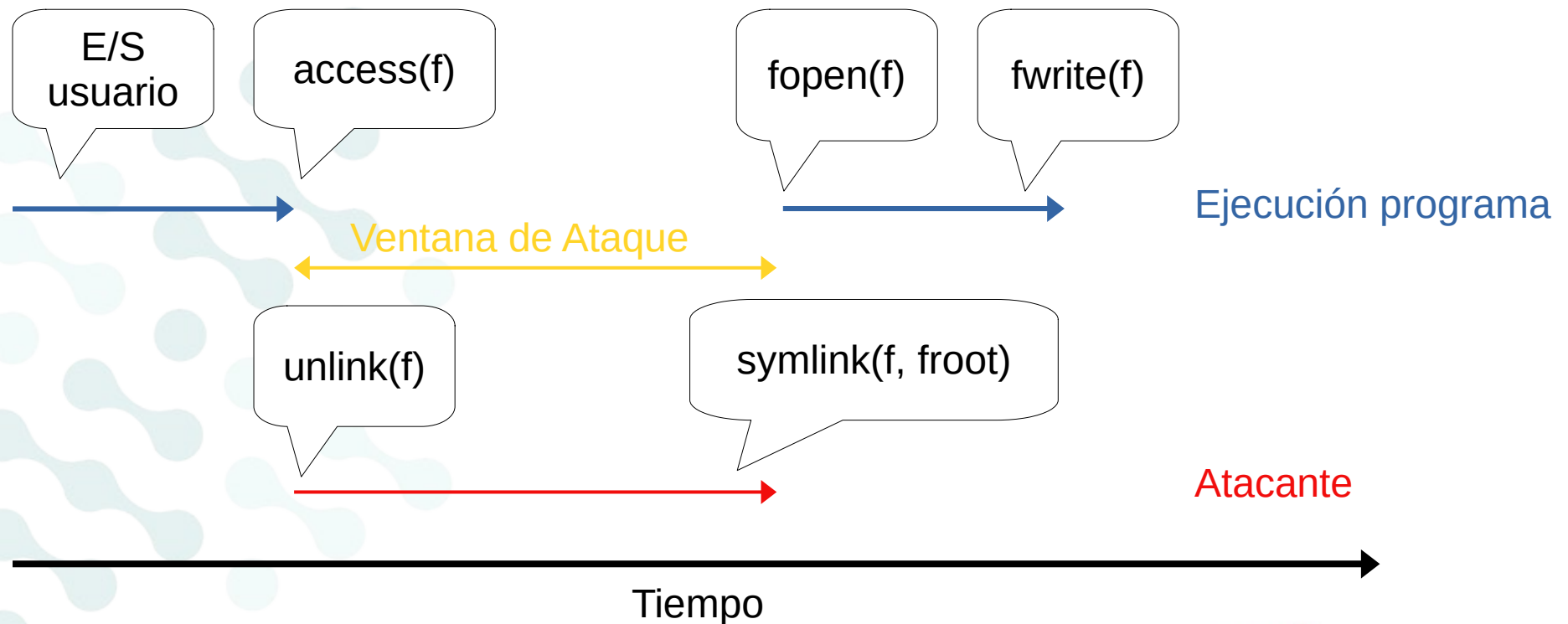
- Objetivo: binario SUID con un TOCTOU

```
1. #include <stdio.h>
2. #include <unistd.h>
3. #include <string.h>
4.
5. int main(int argc, char * argv[])
6. {
7.     char *file = argv[1];
8.     char buffer[51];
9.     FILE *fd;
10.
11.     /* get user input */
12.     scanf("%50s", buffer);
13.
14.     /* check access */
15.     if(!access(file, W_OK)) {
16.         /* write user input to file */
17.         fd = fopen(file, "a+");
18.         fwrite(buffer, sizeof(char), strlen(buffer), fd);
19.         fclose(fd);
20.     } else {
21.         printf("User does not have access\n");
22.     }
23.
24.     return 0;
25. }
```



# Ejemplo de Explotación mediante Symlinks

- Patrón de explotación:



# Ejercicio

- Crear un programa que:
  - Tome como nombre del archivo a editar el primer parámetro de la línea de comandos
  - Defina un texto a escribir en el archivo
  - Verifique permisos del archivo:
    - Si el usuario TIENE permisos:
      - Simule el delay (procesamiento del archivo)
      - Abra el archivo, escriba el mensaje y lo cierre
    - Si el usuario NO TIENE permisos:
      - De un mensaje de error: “Sin permisos”



# Simulación del Delay (aka “procesamiento”)

```
#define DELAY 99999999

/* Simular la demora entre la verificación y la acción */
for(i = 0; i < DELAY; i++) {
    int a = i^2; /* Se podría utilizar cualquier otra operación, es solo un ejemplo */
}
```



# Armado Ambiente de Prueba

- Crear un archivo (no vacío) con el usuario común
- Cambiarle el dueño a root
- Compilar el programa vulnerable
- Cambiarle el dueño a root al programa vulnerable
- Agregar permisos SUID root programa vulnerable
- Dar permisos de ejecución al script de prueba





# Ejecución del Ataque

- Se provee el script exploit-toctou.sh que:
  - Toma como primer parámetro el nombre del programa vulnerable
  - Toma como segundo parámetro el nombre del archivo protegido
  - Lleva adelante el ataque creando el link simbólico y ejecutando el programa vulnerable

**¿Qué pasa si ejecutan múltiples veces seguidas el exploit? ¿Por qué?**



# Ayudas...

- Correr algo como root en Linx  
`sudo comando`
- Hacer SUID un programa en Linux  
`chmod u+s archivo`
- Cambiar dueño de un archivo a root en Linux  
`chown root:root archivo`
- Compilación  
`clang archivo.c -o archivo_ejecutable`



# Ayudas cont.

- Agregar contenido a un archivo  
echo “contenido” > archivo
- Dar permisos de ejecución  
chmod +x archivo

**OJO: ¡Al recompilar repetir  
asignación de permisos!**



# ¡Gracias!

## ¿Preguntas?

[lmeiners@dc.uba.ar](mailto:lmeiners@dc.uba.ar)



DEPARTAMENTO  
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA