TOCTOU attack

find/rm	**Attacker**
	mkdir (“/tmp/badetc”)
	creat (“/tmp/badetc/passwd”)
readdir (“/tmp”) → “badetc”	
lstat (“/tmp/badetc”) → DIRECTORY	
readdir (“/tmp/badetc”) → “passwd”	
	rename (“/tmp/badetc” → “/tmp/x”)
	symlink (“/etc”, “/tmp/badetc”)
unlink (“/tmp/badetc/passwd”)	

Time-of-check-to-time-of-use (a.k.a TOCTOU) bug

- find checks that `/tmp/badetc` is not symlink
- but meaning of file name changes before it is used

Another example - xterm

`xterm` Provides a terminal window in X-windows - used to run with setuid root privileges

- Requires kernel pseudo-terminal (`pty`) device
- Required root privileges to change ownership of `pty` to user
- Also writes protected `utmp`/`wtmp` files to record users

Had feature to log terminal session to file

```
if (access (logfile, W_OK) < 0)
  return ERROR;

fd = open (logfile, O_CREAT|O_WRONLY|O_TRUNC, 0666);
/* ... */
```

➡ `xterm` is root, but should not log to file user cannot write

✓ `access` call does permission check with real, not effective UID

◉ .... but another TOCTOU bug