

Another TOCTOU attack

xterm

access (“/tmp/log”) → OK

open (“/tmp/log”)

Attacker

creat (“/tmp/log”)

unlink (“/tmp/log”)

symlink (“/tmp/log” → “/etc/passwd”)

Attacker changes /tmp/log between check and use

➡ xterm unwittingly overwrites /etc/passwd

- OpenBSD man page - "CAVEATS : access() is a potential security hole and should never be used."

Preventing TOCTOU

- ➔ Use new APIs that are relative to an opened directory file descriptor
 - `openat`, `renameat`, `unlinkat`, `symlinkat`, `faccessat`
 - `fchown`, `fchownat`, `fchmod`, `fchmodat`, `fstat`, `fstatat`
 - `O_NOFOLLOW` flag to `open` avoids symbolic links in last component
- But can still have TOCTOU problems with hardlinks
- ✓ Alternative solution - lock resources, though most systems only lock files (and locks are typically advisory)
- ✓ Alternative solution - wrap groups of operations in OS transactions
e.g. Microsoft supports for transactions on Windows Vista and newer
`CreateTransaction`, `CommitTransaction`, `RollbackTransaction`