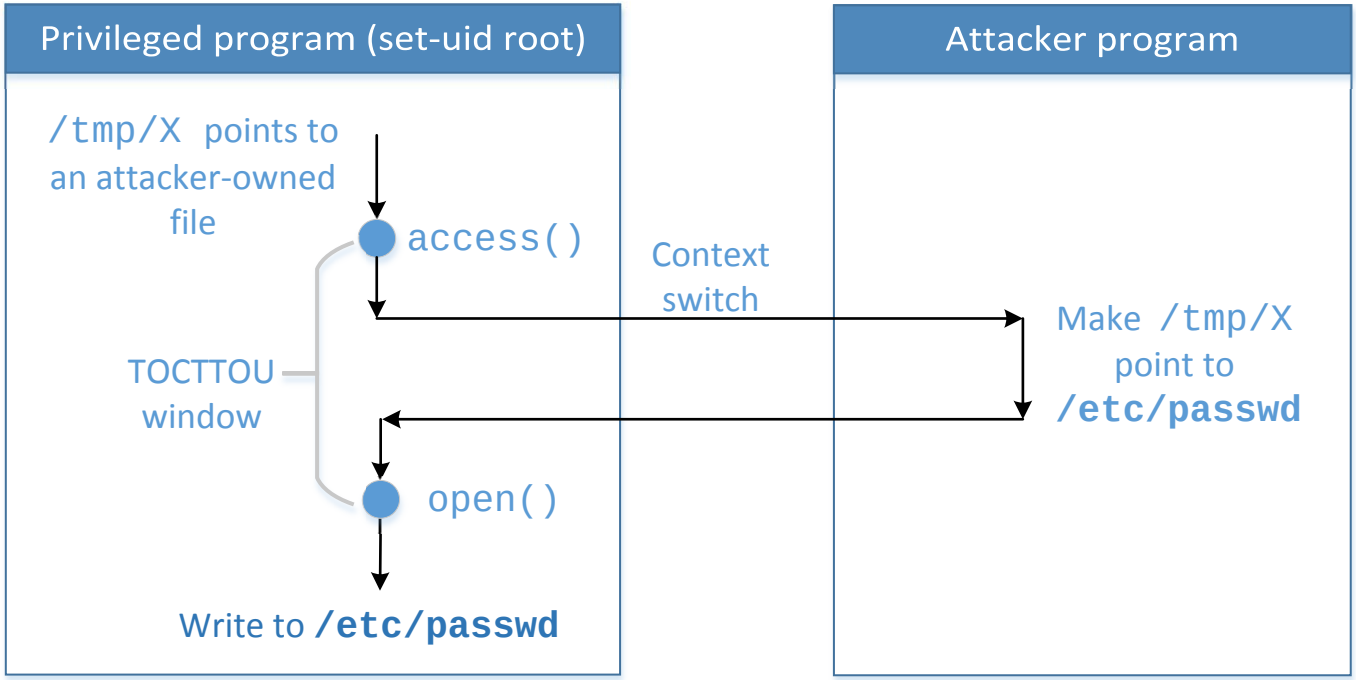
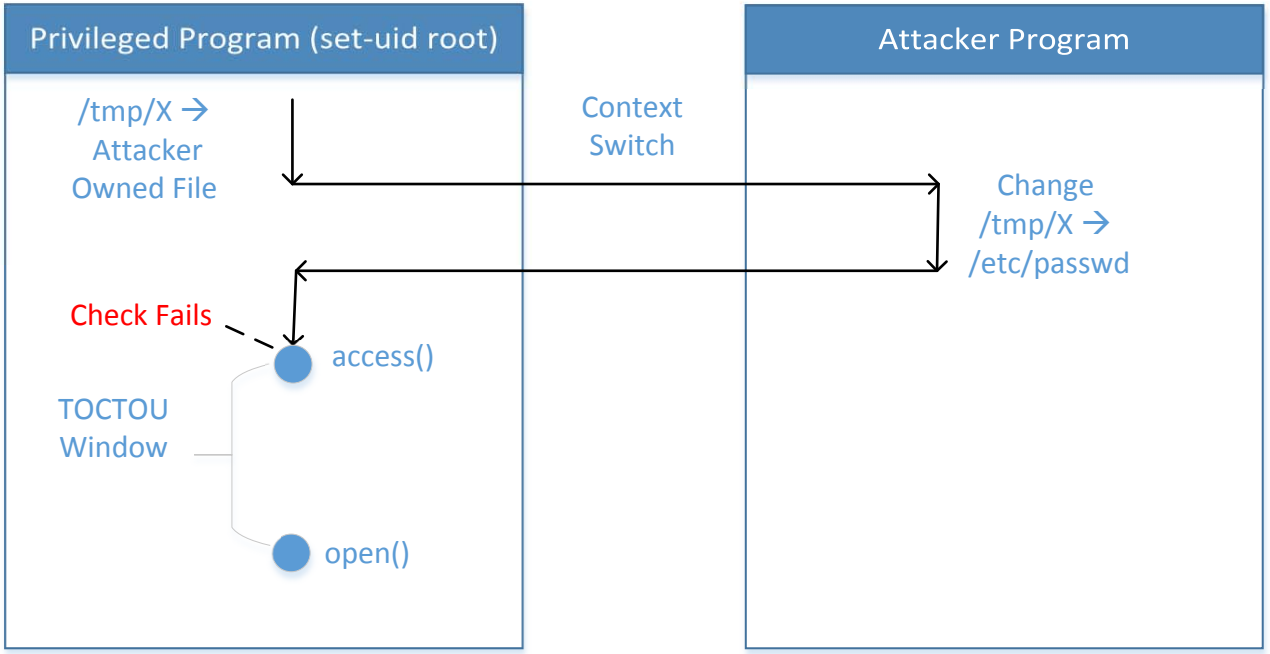
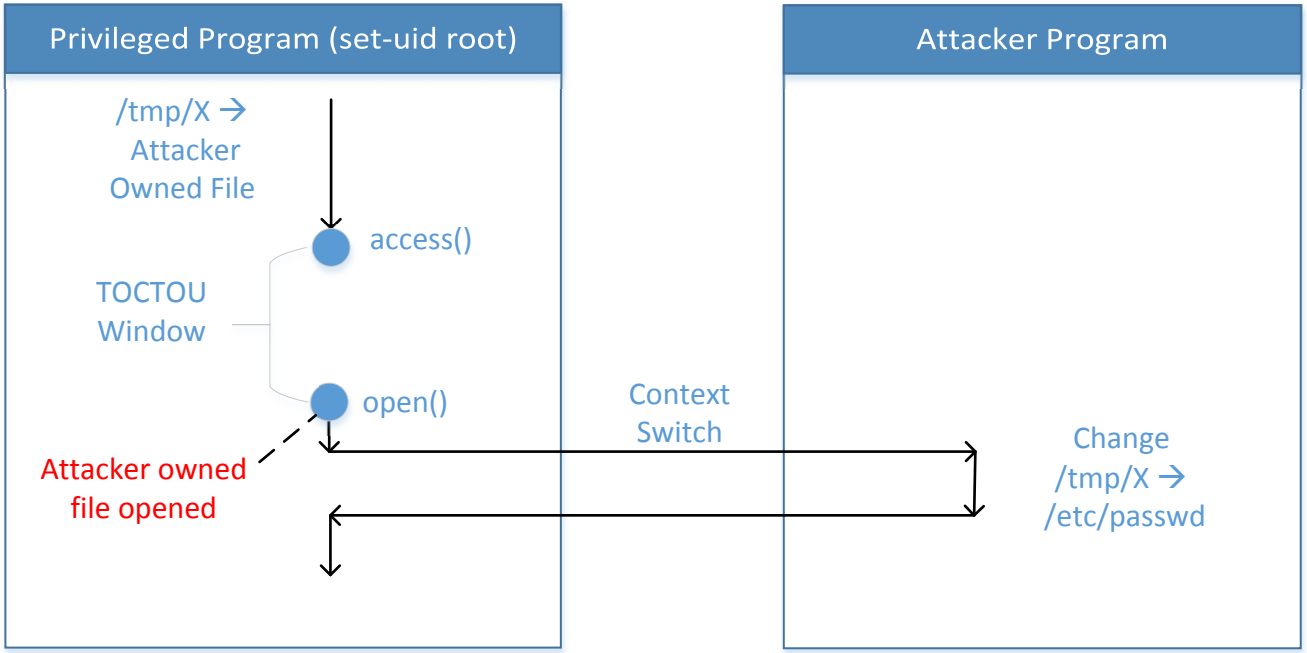
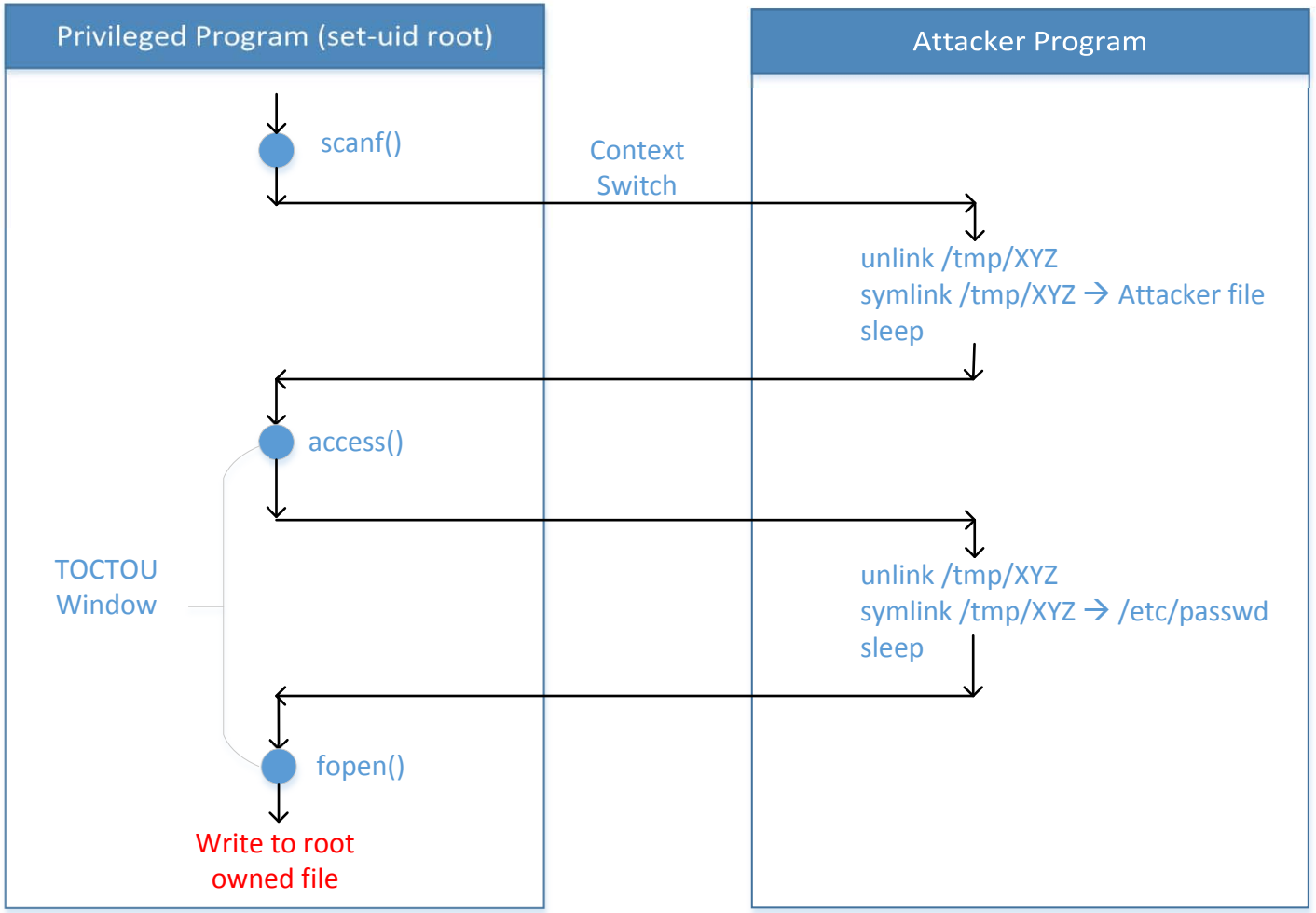

Privileged program (set-uid root)
Attacker program
/tmp/X points to an attacker-owned file
access()
Context switch
Make /tmp/X point to /etc/passwd
TOCTTOU window
open()
Write to /etc/passwd


Privileged Program (set-uid root)
Attacker Program
/tmp/X → Attacker Owned File
Context Switch
Change /tmp/X → /etc/passwd
Check Fails
access()
TOCTOU Window
open()


Privileged Program (set-uid root)
Attacker Program
/tmp/X → Attacker Owned File
access()
TOCTOU Window
open()
Attacker owned file opened
Context Switch
Change /tmp/X → /etc/passwd


Privileged Program (set-uid root)
Attacker Program
scanf()
Context Switch
unlink /tmp/XYZ
symlink /tmp/XYZ → Attacker file
sleep
access()
TOCTOU Window
unlink /tmp/XYZ
symlink /tmp/XYZ → /etc/passwd
sleep
fopen()
Write to root owned file