A TOCTOU attack in 3 steps

I.The innocent user creates a file

2. The innocent users invokes a program executed with higher privileges to use this file

3. The (not so) innocent user swapped the file with another one that he or she has not the right to access

➤ The sequence of events requires precise timing

✓ Possible for an attacker to arrange such conditions (race condition)

A TOCTOU attack in 3 steps

1. The innocent user creates a file
2. The innocent users invokes a program executed with higher privileges to use this file
3. The (not so) innocent user swapped the file with another one that he or she has not the right to access

➡ The sequence of events requires precise timing

✓ Possible for an attacker to arrange such conditions (race condition)

The printer attack on Unix

Bob

admin (root)