

# Let us look at the system calls

## **find/rm**

---

```
readdir (“/tmp”) → “badetc”  
lstat (“/tmp/badetc”) → DIRECTORY  
readdir (“/tmp/badetc”) → “passwd”
```

```
unlink (“/tmp/badetc/passwd”)
```

## **Attacker**

---

```
mkdir (“/tmp/badetc”)  
creat (“/tmp/badetc/passwd”)
```

# TOCTOU attack

## **find/rm**

---

```
readdir (“/tmp”) → “badetc”  
lstat (“/tmp/badetc”) → DIRECTORY  
readdir (“/tmp/badetc”) → “passwd”  
  
unlink (“/tmp/badetc/passwd”)
```

## **Attacker**

---

```
mkdir (“/tmp/badetc”)  
creat (“/tmp/badetc/passwd”)  
  
rename (“/tmp/badetc” → “/tmp/x”)  
symlink (“/etc”, “/tmp/badetc”)
```

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