Kerberos Vulnerability

Based on presentation in
”The art of software security assessment”
Dowd, McDonald, Schuh

Kerberos 4 code

```
errno = 0
if (lstat(file, &statb) < 0)
  goto out;

if (!(statb.st_mode & S_IFREG)
#ifdef notdef
  || statb.st_mode & 077
#endif
  )
  goto out;

if ((fd = open(file, O_RDWR|O_SYNC,0)) <0)
  goto out;
```

Kerberos 4 code

```
errno = 0
if (lstat(file, &statb) < 0)
  goto out;

if (!(statb.st_mode & S_IFREG)
#ifdef notdef
  || statb.st_mode & 077
#endif
  )
```

This code is run by a privileged login daemon

➔ what if attacker has replaced the ”regular file” with a symbolic link pointing somewhere else in the system?

Kerberos 4 code

```
errno = 0
if (lstat(file, &statb) < 0)
#ifdef notdef
  || statb.st_mode & 077
#endif
  )
```

lstat = return information about a file:
is this a regular file?

This code is run by a privileged login daemon
➔ what if attacker has replaced the ”regular file” with a symbolic link pointing somewhere else in the system?

Kerberos 4 code

```
errno = 0
if (lstat(file, &statb) < 0)
  goto out;
```

```
if (!(statb.st_mode & S_IFREG)
#ifdef notdef
  || statb.st_mode & 077
#endif
  )
  goto out;

if ((fd = open(file, O_RDWR|O_SYNC,0)) <0)
  goto out;
```

Kerberos 4 code

```
errno = 0
if (lstat(file, &statb) < 0)
  goto out;
```

```
if (!(statb.st_mode & S_IFREG)
#ifdef notdef
  || statb.st_mode & 077
#endif
  )
  goto out;
```

```
if ((fd = open(file, O_RDWR|O_SYNC,0)) <0)
  goto out;
```

Kerberos 4 code

```
errno = 0
if (lstat(file, &statb) < 0)
  goto out;

if (!(statb.st_mode & S_IFREG)
#ifdef notdef
  || statb.st_mode & 077
#endif
  )
  goto out;

if ((fd = open(file, O_RDWR|O_SYNC,0)) <0
  goto out;
```

Regular file, so safe to open?

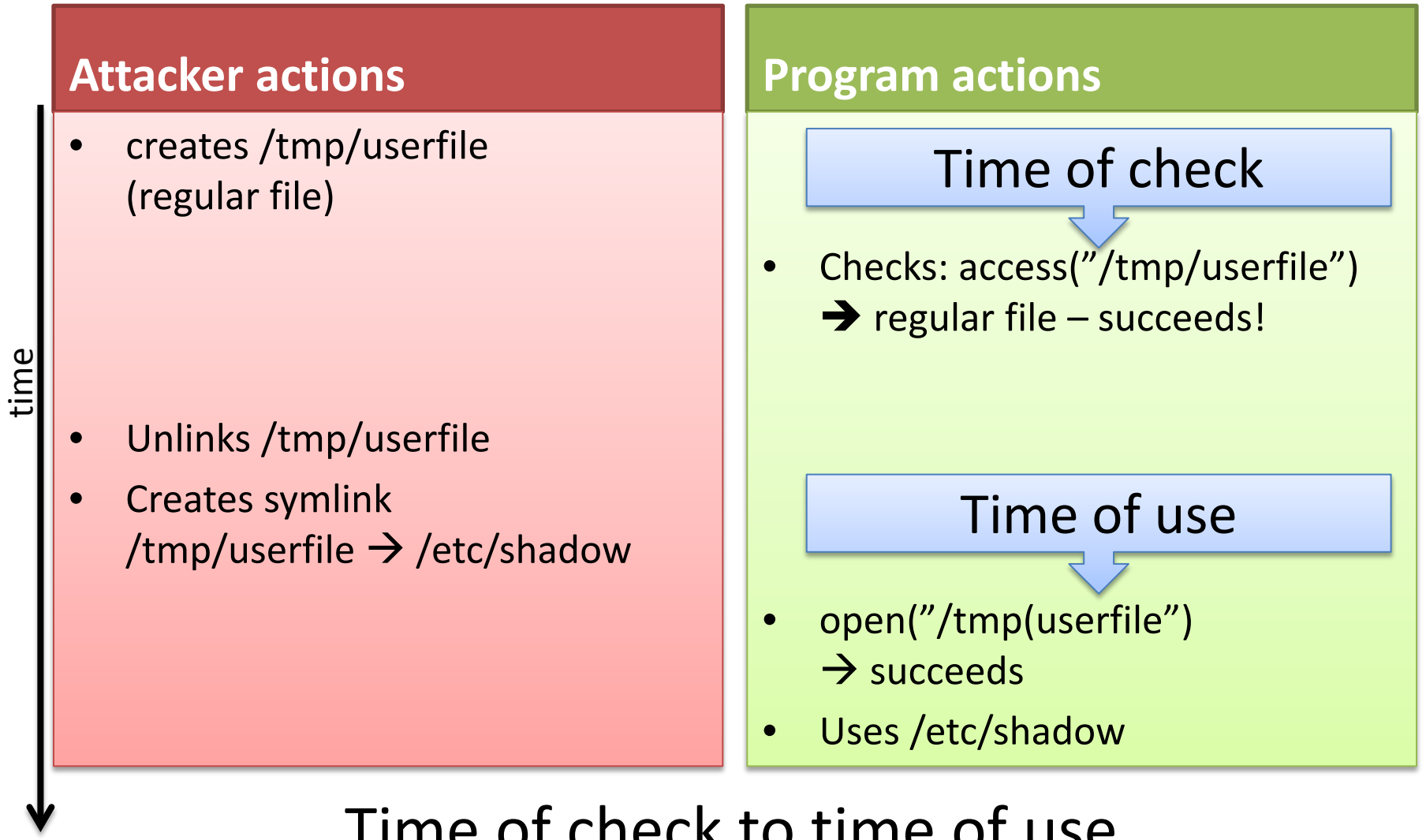
TOCTOU flaw

time

Attacker actions	Program actions
• creates /tmp/userfile (regular file)	• Checks: access("/tmp/userfile") ➔ regular file – succeeds!
• Unlinks /tmp/userfile • Creates symlink /tmp/userfile → /etc/shadow	• open("/tmp(userfile") → succeeds • Uses /etc/shadow

Time of check to time of use

TOCTOU flaw



Time of check to time of use