

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)
```

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

```
#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)
    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

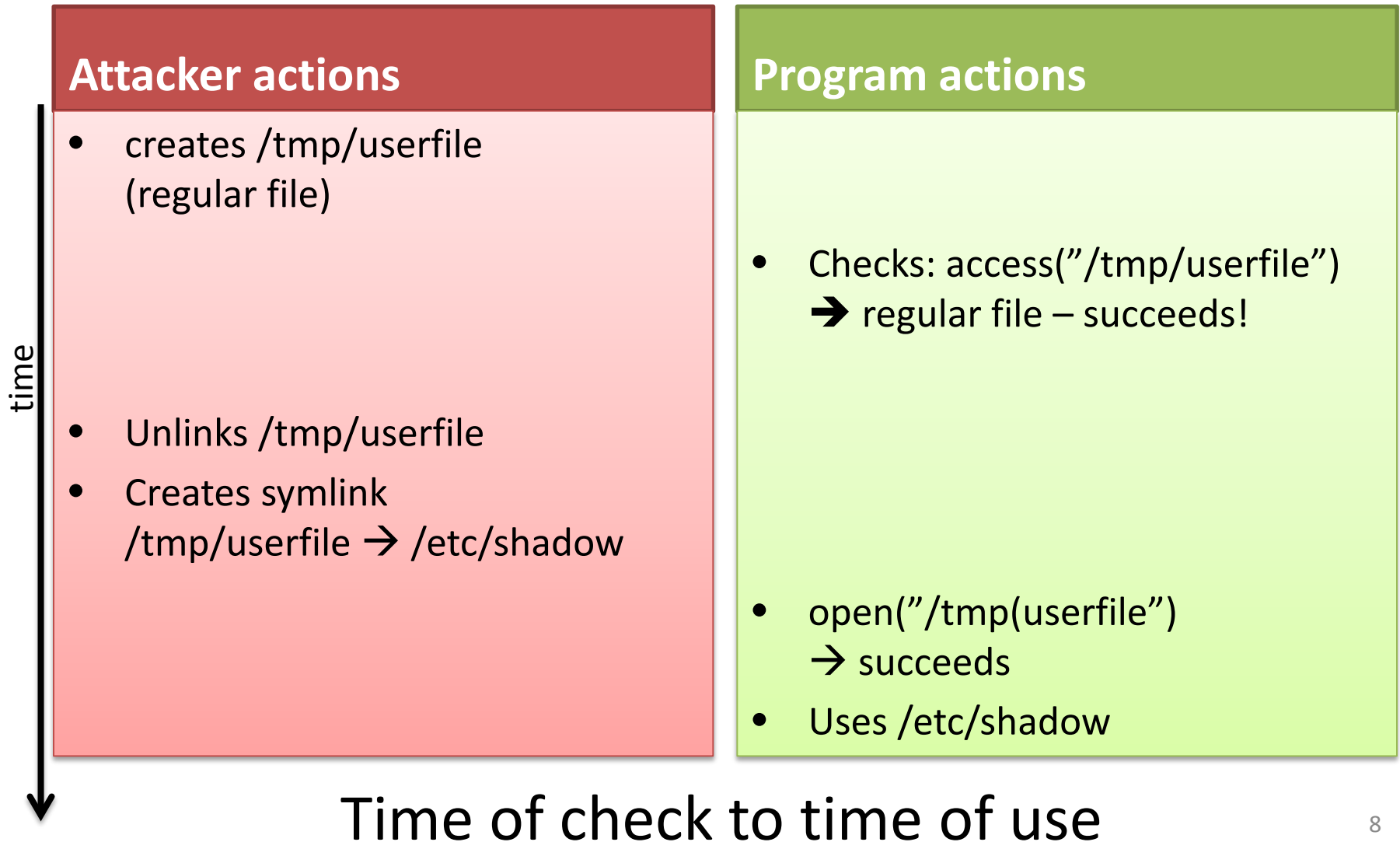
```
errno = 0
if (lstat(file, &statb) < 0)
    goto out;

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



TOCTOU flaw

