Kerberos Vulnerability

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

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

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

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

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?

3

```
errno = 0
if (lstat(file, &statb) < 0)</pre>
Istat = 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?

4

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

```
errno = 0
if (lstat(file, &statb) < 0)</pre>
  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)</pre>
```

goto out;

```
errno = 0
if (lstat(file, &statb) < 0)</pre>
  goto out;
if (!(statb.st_mode & S_IFREG)
#ifdef notdef
  || statb.st_mode & 077
#endif
  goto out;
                                              Regular file, so
if ((fd = open(file, O_RDWR|O_SYNC,0)) <0 safe to open?
  goto out;
```

- Unlinks /tmp/userfile
- Creates symlink
 /tmp/userfile → /etc/shadow

Program actions

- Checks: access("/tmp/userfile")
 - → regular file succeeds!

- open("/tmp(userfile")
 - → succeeds
- Uses /etc/shadow

tim

Time of check to time of use

TOCTOU flaw

Attacker actions

creates /tmp/userfile (regular file)

- Unlinks /tmp/userfile
- Creates symlink
 /tmp/userfile → /etc/shadow

Program actions

Time of check

- Checks: access("/tmp/userfile")
 - → regular file succeeds!

Time of use

- open("/tmp(userfile")
 - → succeeds
- Uses /etc/shadow

time

Time of check to time of use