University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Race condition: Examples
Access System Call

bristol.ac.uk

Exampe 1: access system call

```
if(access(“/tmp/X”, W_OK)) {
        f = open(“tmp/X”);
        write_to_file(f);
} else {
        printf(“You do not own the file”);
}
```

Exampe 1: access system call

```
if(access("/tmp/X", W_OK)) {
        f = open("tmp/X");
        write_to_file(f);
} else {
        printf("You do not own the
        file");
}
```

- setuid: root
- want to make sure the "real" user own the file

Exampe 1: access system call

```
if(access(“/tmp/X”, W_OK)) {
        f = open(“tmp/X”);
        write_to_file(f);
} else {
        printf(“You do not own the
        file”);
}
```

- setuid: root
- want to make sure the “real” user own the file
- access return either or not the operation is permitted to current user

University of BRISTOL

How can this be exploited?

bristol.ac.uk

Exampe 1: access system call

```
if(access(“/tmp/X”, W_OK)) {
        f = open(“tmp/X”);
        write_to_file(f);
} else {
        printf(“You do not own the
        file”);
}
```

- Path hard coded
  - Program will only write to /tmp/X

Exampe 1: access system call

```
if(access(“/tmp/X”, W_OK)) {        1
        f = open(“tmp/X”);          2
        write_to_file(f);
} else {
        printf(“You do not own the
        file”);
}
```

- Path hard coded
  - Program will only write to /tmp/X
- Symbolic Link
  - /tmp/X -> /etc/config
- 1: fail
- 2: success

Exampe 1: access system call

```
if(access(“/tmp/X”, W_OK)) {        1
        f = open(“tmp/X”);          2
        write_to_file(f);
} else {
        printf(“You do not own the
        file”);
}
```

- Exploited race condition
- Changed value between check and use
- time of check to time of use
  - TOCTOU

access man

Warning: Using **access**() to check if a user is authorized to, for example, open a file before actually doing so using ***open****(2)* creates a security hole, because the user might exploit the short time interval between checking and opening the file to manipulate it. **For this reason, the use of this system call should be avoided**. (In the example just described, a safer alternative would be to temporarily switch the process's effective user ID to the real ID and then call ***open****(2)*.)