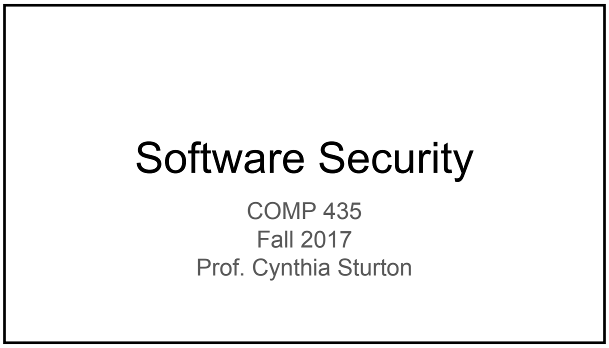
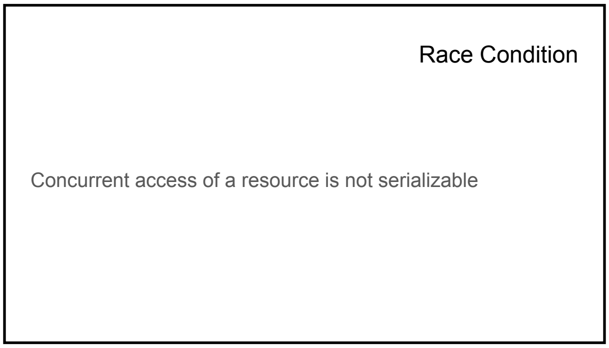


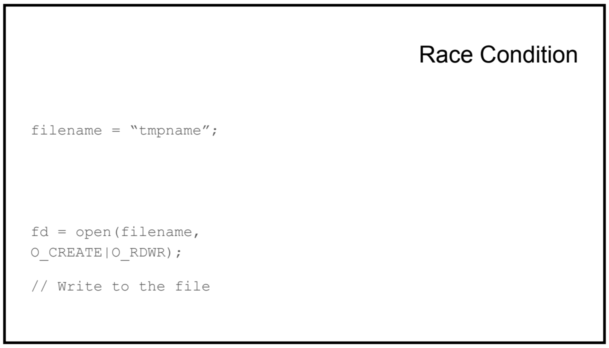
Software Security

COMP 435
Fall 2017
Prof. Cynthia Sturton



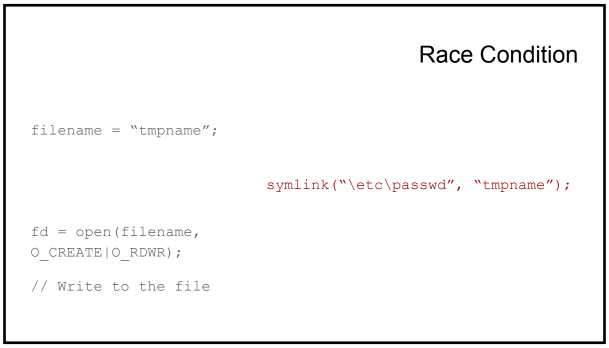
Race Condition

Concurrent access of a resource is not serializable



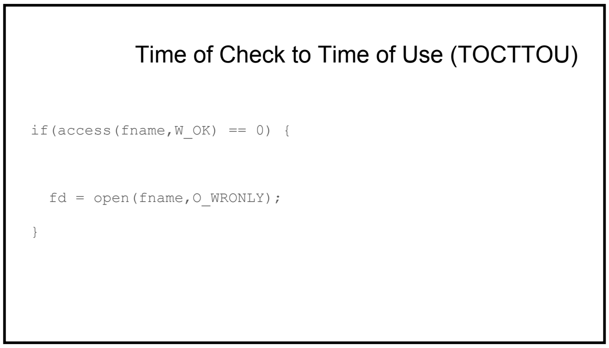
Race Condition

```
filename = “tmpname”;



fd = open(filename,
O_CREATE|O_RDWR);

// Write to the file
```



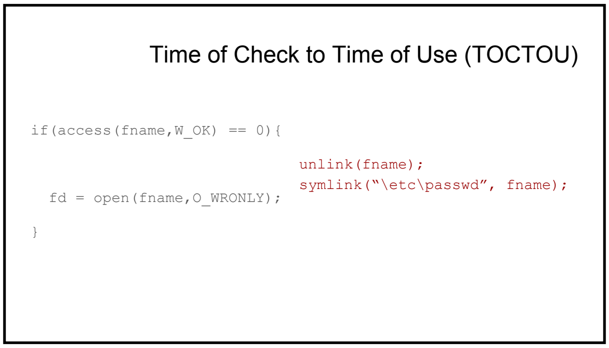
Race Condition

```
filename = “tmpname”;

                          symlink(“\etc\passwd”, “tmpname”);

fd = open(filename,
O_CREATE|O_RDWR);

// Write to the file
```



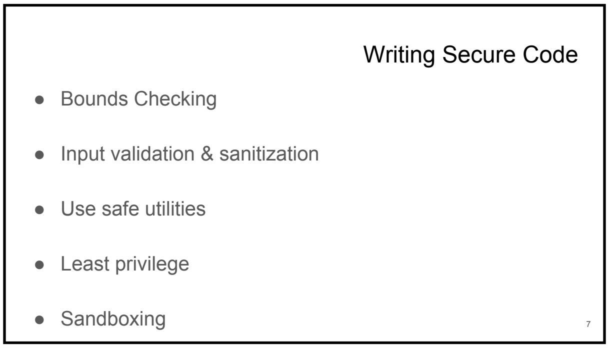
Time of Check to Time of Use (TOCTTOU)

```
if(access(fname,W_OK) == 0) {

  fd = open(fname,O_WRONLY);
}
```



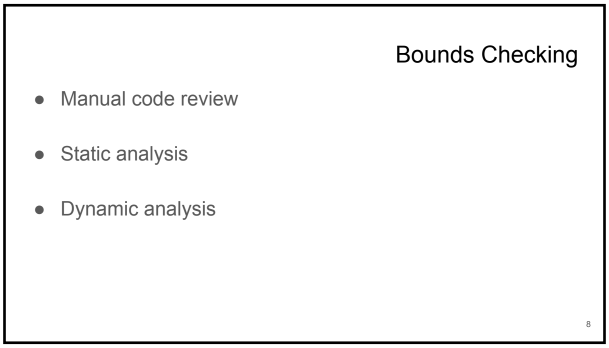
Time of Check to Time of Use (TOCTOU)

```
if(access(fname,W_OK) == 0){
                              unlink(fname);
                              symlink(“\etc\passwd”, fname);
  fd = open(fname,O_WRONLY);
}
```



Writing Secure Code

- Bounds Checking
- Input validation & sanitization
- Use safe utilities
- Least privilege
- Sandboxing



Bounds Checking

- Manual code review
- Static analysis
- Dynamic analysis

Input Validation & Sanitization

- Use a template

    (919) 555-1234

Input Validation & Sanitization

- Use a template

    (919) 555-1234

- Templates prescribe good behavior

Templates are Difficult

(919) 555-1234

1-919-555-1234

+1 919 555 1234

919 555 1234

919.555.1234

Input Validation & Sanitization

The length of buffer writes should be dictated by buffer size, not by user-provided input

Input Validation & Sanitization

Never trust user-supplied input

Use Safe Utilities

strcpy vs strncpy

```
char str1[]= "hello";
char str2[5];

/* copy to terminating null ‘\0’ */
  strcpy (str2, str1);

/* copy only 5 chars */
  strncpy (str2, str1, 5);
```

Use Safe Utilities

- strcpy vs strncpy
- strcmp vs strncmp
- sprintf vs snprintf

Least Privilege

Subject should have access to fewest number of objects necessary to do its work

Least Privilege

- Code should have only the permissions needed
- Limits the damage done by compromise

Sandboxing

Contain sections of code within a specified address range

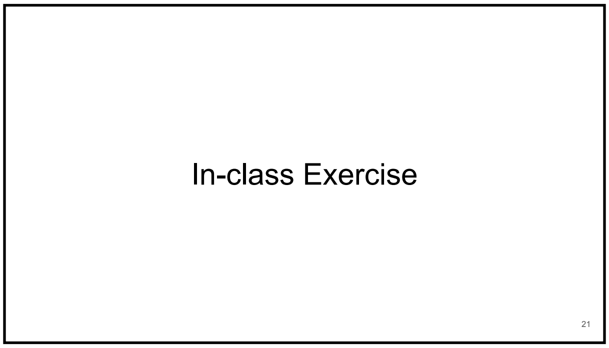
Programming Language

The choice of language plays a role as well

- Memory Safety
- Type Safety

Security and Software Engineering

Security best practice $\supseteq$ Software engineering best practice



In-class Exercise