University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Race condition: Examples
Reference Monitor

bristol.ac.uk

University of BRISTOL

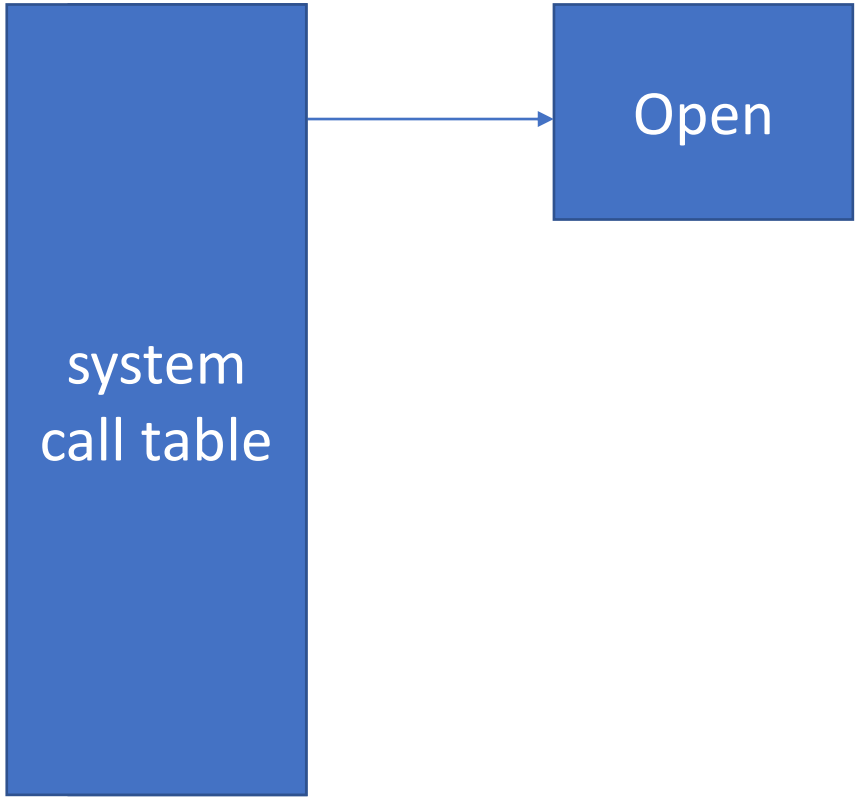
What is a reference monitor?

bristol.ac.uk

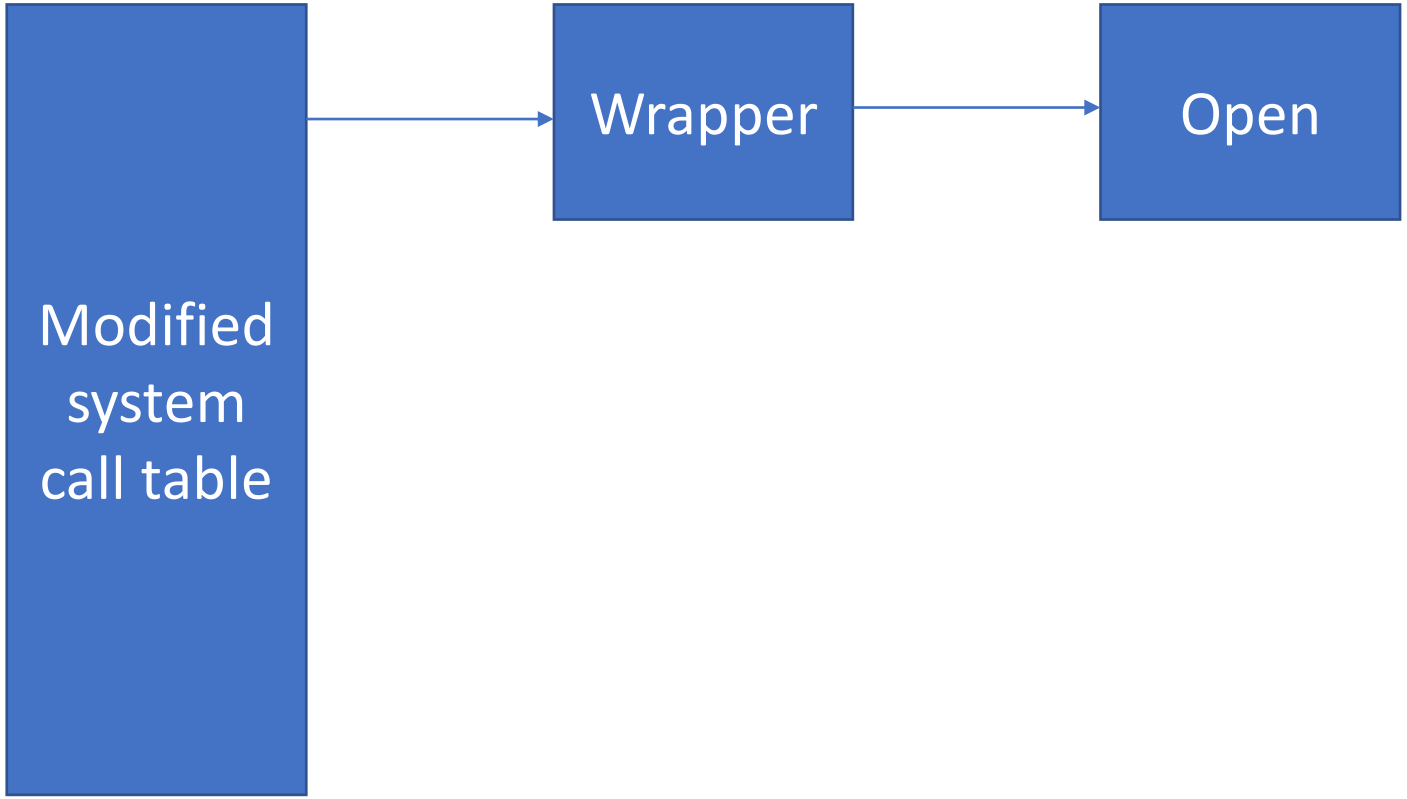
Example 2: implementing OS reference monitor

- *a **reference monitor** is a secure, always-used and fully-testable module that controls all software access to data objects or devices*

Example 2: implementing OS reference monitor

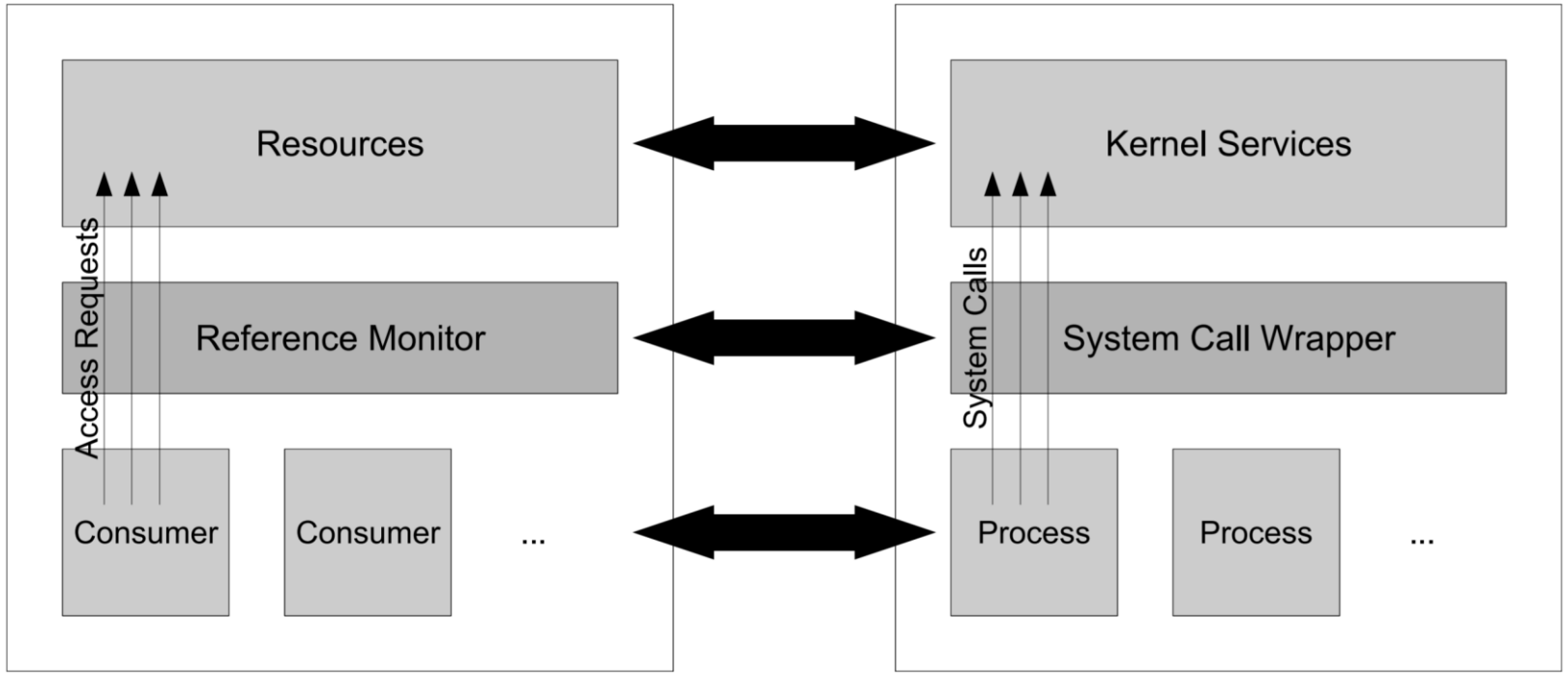


Example 2: implementing OS reference monitor

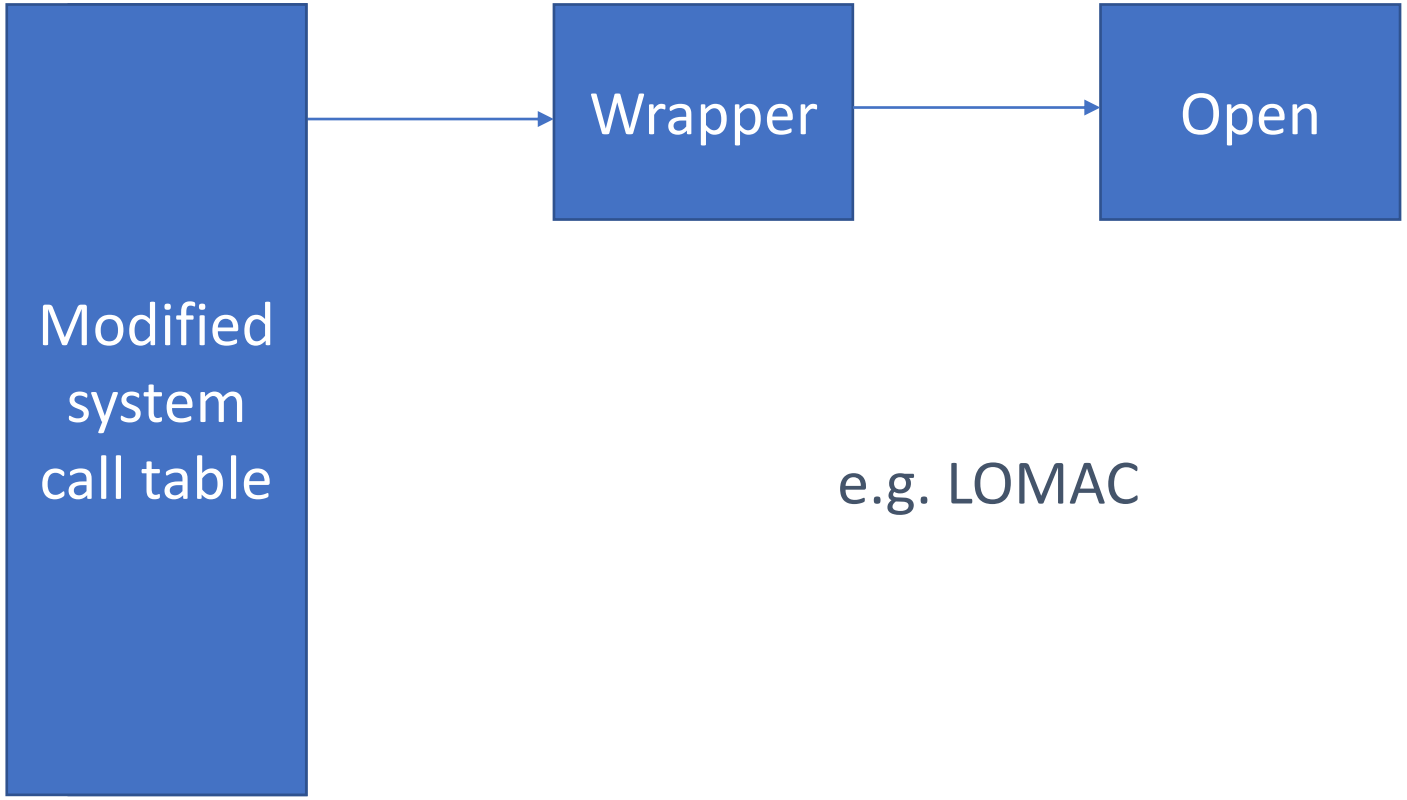


Example 2: implementing OS reference monitor

- *a **reference monitor** is a secure, always-used and fully-testable module that controls all software access to data objects or devices*

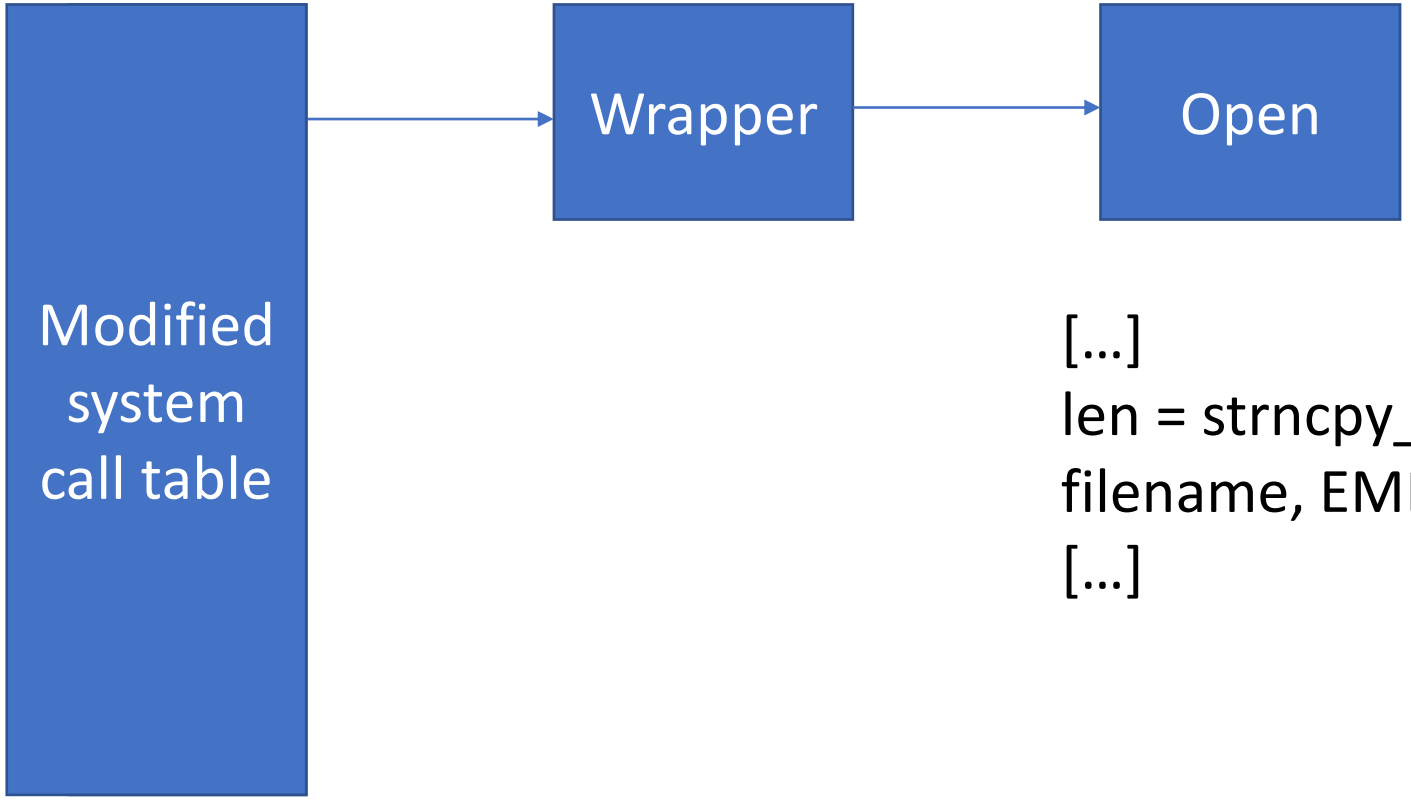


Example 2: implementing OS reference monitor



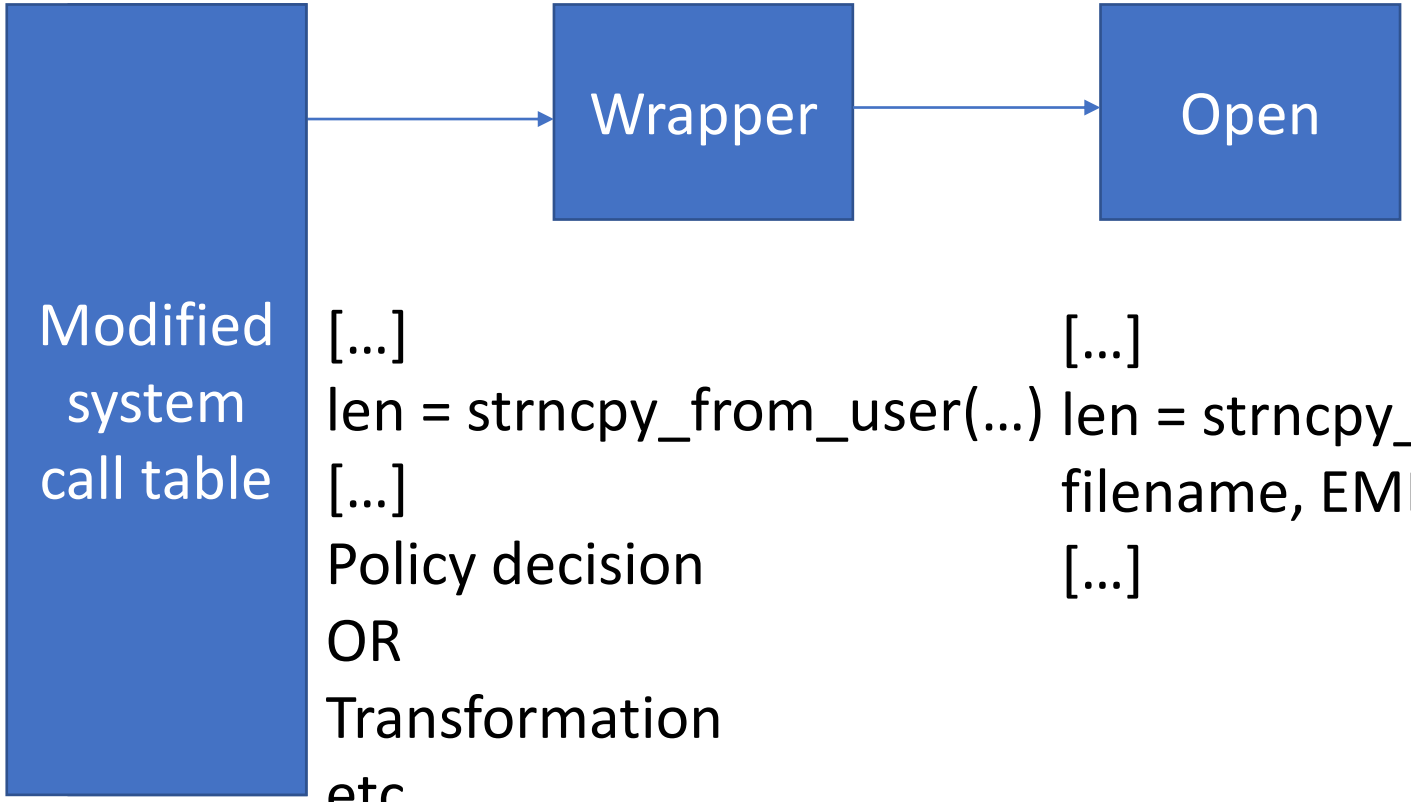
e.g. LOMAC

Example 2: implementing OS reference monitor




```
[…]
len = strncpy_from_user(kname,
filename, EMBEDDED_NAME_MAX);
[…]
```

Example 2: implementing OS reference monitor



University of BRISTOL

Problem?

bristol.ac.uk

Example 2: implementing OS reference monitor

- Wrapper and syscall work on two different copy of the buffer!
- User space controlled buffer
  - Can be controlled by an attacker
- The value checked to enforce policy!=value seen by syscall

Example 2: implementing OS reference monitor

- Wrapper and syscall work on two different copy of the buffer!
- User space controlled buffer
  - Can be controlled by an attacker
- The value checked to enforce policy!=value seen by syscall
- We will discuss how Linux implement its reference monitor in a future video

Example 2: implementing OS reference monitor

- Wrapper and syscall work on two different copy of the buffer!
- User space controlled buffer
  - Can be controlled by an attacker
- The value checked to enforce policy!=value seen by syscall
- We will discuss how Linux implement its reference monitor in a future video
- Check Robert Watson paper for more in depth discussion on this topic