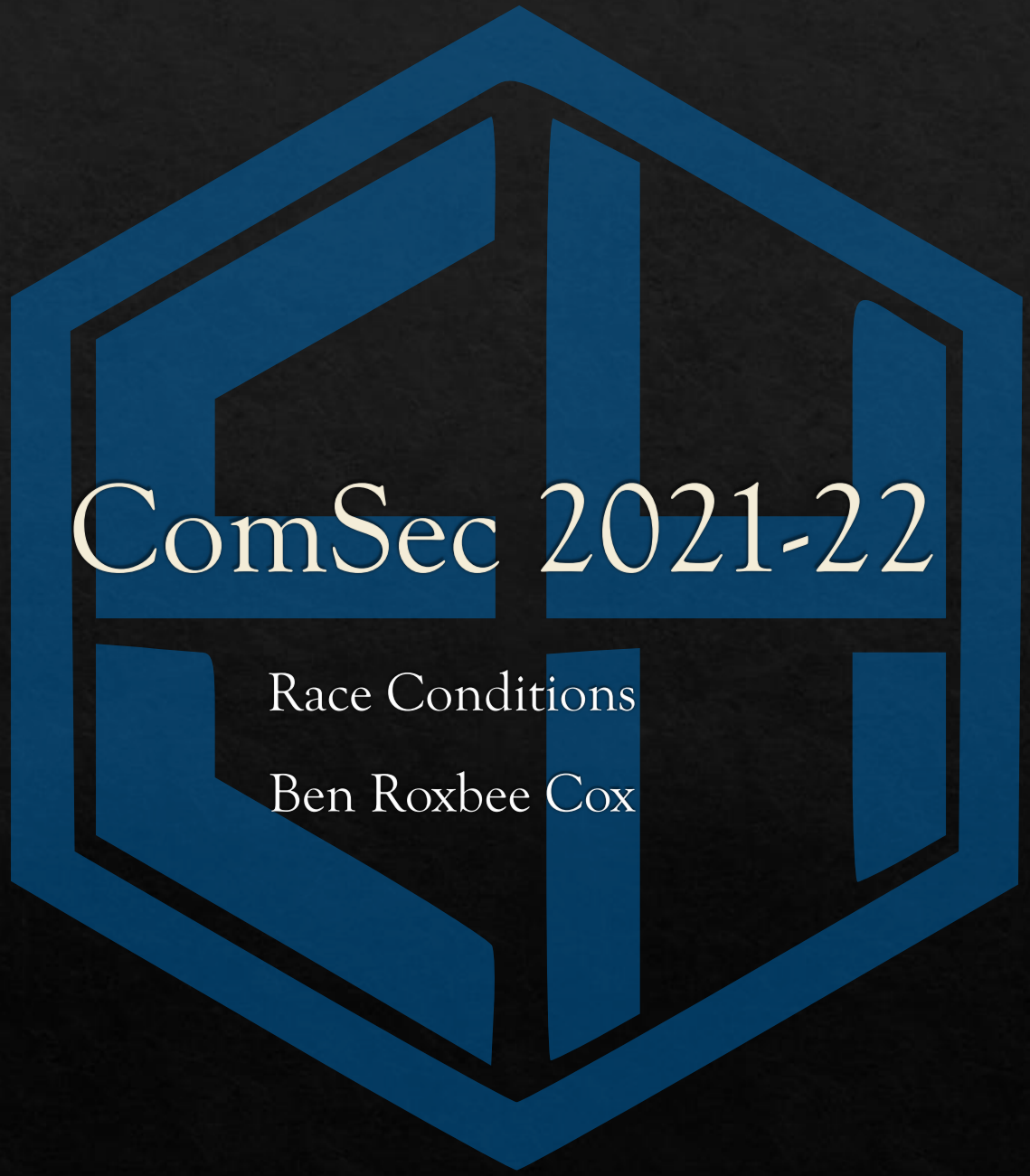

ComSec 2021-22

Race Conditions

Ben Roxbee Cox

Session Format

- Brief introduction to race conditions
- Attempt challenge 0
  - Walkthrough challenge 0
- Attempt challenge 1
  - Walkthrough challenge 1
- Attempt Challenge 2
  - Walkthrough challenge 2

What is a race condition?

- The term *race condition* was already in use by 1954, for example in David A. Huffman's doctoral thesis "The synthesis of sequential switching circuits“.
- Most computers can’t really multi task (much).
- We can exploit the fact that a program must complete a task in a defined sequence of steps.
- Race conditions can be implementation specific. A “secure” program may be vulnerable when implemented into a different system.
- Many processes many use on a single resourse

Order of Process Execution

P1 initialise()
P1 check_input()
P1 do_action()
P1 check_input()
P1 do_action()
P1 terminate()
P2 initialise()
P2 check_input()
P2 do_action()
P2 check_input()
P2 do_action()
P2 terminate()

P1 initialise()
P2 initialise()
P1 check_input()
P2 check_input()
P1 do_action()
P2 do_action()
P1 check_input()
P2 check_input()
P1 do_action()
P2 do_action()
P1 terminate()
P2 terminate()

P1 initialise()
P1 check_input()
P2 initialise()
P2 check_input()
P2 do_action()
P2 check_input()
P2 do_action()
P2 terminate()
P1 do_action()
P1 check_input()
P1 do_action()
P1 terminate()

P1 initialise()
P2 initialise()
P2 check_input()
P1 check_input()
P1 do_action()
P1 check_input()
P2 do_action()
P1 do_action()
P2 check_input()
P2 do_action()
P2 terminate()
P1 terminate()

TOCTOU

- Time-of-Check, Time-of-Use