

1. a) Yes, they are part of system call's Application Programming Interface, and they are the only way to interact between computer program and OS kernel.

### Correct Solution

A system call traps into the kernel so that privileged instruction can be run. A function call jumps into another instruction in user-mode

### Notes

- **Function Call**
  - jumps into another instruction in user mode
- **System Calls**
  - Is issued by a client
  - traps into the kernel so that privileged instruction can be run
  - Is the only entry points into the kernel system
  - Provides services via API or Application Program Interface
  - Has five different types of calls

Types of System Calls	Windows	Linux
Process Control	CreateProcess() ExitProcess() WaitForSingleObject()	fork() exit() wait()
File Management	CreateFile() ReadFile() WriteFile() CloseHandle()	open() read() write() close()
Device Management	SetConsoleMode() ReadConsole() WriteConsole()	ioctl() read() write()
Information Maintenance	GetCurrentProcessID() SetTimer() Sleep()	getpid() alarm() sleep()
Communication	CreatePipe() CreateFileMapping() MapViewOfFile()	pipe() shmget() mmap()

### Example

`open()`, `read()`, `write()`, `close()`, `mkdir()` are other examples of system calls

### References

- 1) Tutorials Point, Types of System Calls, link

- b) It is user's responsibility to keep track of allocated blocks of heap memory, and memory leak occurs if user fails to deallocate allocated blocks of heap memory

### Notes

- **Memory API**

- Has two types of memory

1. **Stack**

- \* Is also called **automatic memory**
- \* Allocations and deallocations are managed by compiler
- \* Deallocates memory by the end of function call

2. **Heap**

- \* Is long-lived
- \* Allocation and deallocation are managed by user
- \* Creates **memory leak** if memory not freed
- \* **valgrind** is a useful heap memory debugging tool link

- `malloc()`

- \* Is a C library call
- \* **Syntax:** `void *malloc(size_t size)`
- \* Allocates a block of `size` bytes to **heap memory** and if successful, returns a pointer to it
- \* Returns `NULL` if memory allocation is unsuccessful

### Example

```
int *x = malloc(10 * sizeof(int));
```

- `free()`

- \* Is a C library call
- \* Frees heap memory that is no longer in use

### Example

```
int *x = malloc(10 * sizeof(int));  
...  
free(x);
```


- `brk()`, `sbrk()`, `mmap()`

- \* Are system calls for memory management

- **Buffer overflow**

- is an error that occurs when not enough heap memory is allocated

Missing + 1



```
char *src = "hello";
char *dst = (char *) malloc(strlen(src)); // too small!
strcpy(dst, src); // work properly
```

- c) If the access by two threads are both about reading the stored value (as opposed to write), then concurrency error will not occur.
- d) Hand-over-hand locking is a fine-grained-locking, which allows more threads to be locked at once than single lock, and this means it will perform better than single lock when there is a lot of contention,

### Notes

- **Coarse-grained-locking**

- Is one big lock that is used any time any critical section is accessed
- Is easy to write
- Is easy to prove correctness
- No fault-tolerance but deadlock-free
- Performs poorly when contention (the need for performance due to load) is high
- \* No concurrent access

### Example

```
pthread_mutex_t lock = PTHREAD_MUTEX_INITIALIZER;
pthread_cond_t cond = PTHREAD_COND_INITIALIZER;

pthread_mutex_lock(&lock);
while (ready == 0)
    pthread_cond_wait(&cond, &lock);
pthread_mutex_unlock(&lock);
```

One lock for all threads  
(coarse-grained lock)

Notice that only one thread  
can pass at a time

- **Fine-grained-locking**

- Uses different locks to often protect different data and data structures
- Allows more threads to be in locked code at once

### Example

```

1 void List_Init(list_t *L) {
2     L->head = NULL;
3     pthread_mutex_init(&L->lock, NULL);
4 }
5
6 void List_Insert(list_t *L, int key) {
7     // synchronization not needed
8     node_t *new = malloc(sizeof(node_t));
9     if (new == NULL) {
10         perror("malloc");
11         return;
12     }
13     new->key = key;
14
15     // just lock critical section
16     pthread_mutex_lock(&L->lock);
17     new->next = L->head;
18     L->head = new;
19     pthread_mutex_unlock(&L->lock);
20 }
21
22 int List_Lookup(list_t *L, int key) {
23     int rv = -1;
24     pthread_mutex_lock(&L->lock);
25     node_t *curr = L->head;
26     while (curr) {
27         if (curr->key == key) {
28             rv = 0;
29             break;
30         }
31         curr = curr->next;
32     }
33     pthread_mutex_unlock(&L->lock);
34     return rv; // now both success and failure
35 }

```

Fine-grained lock here :)

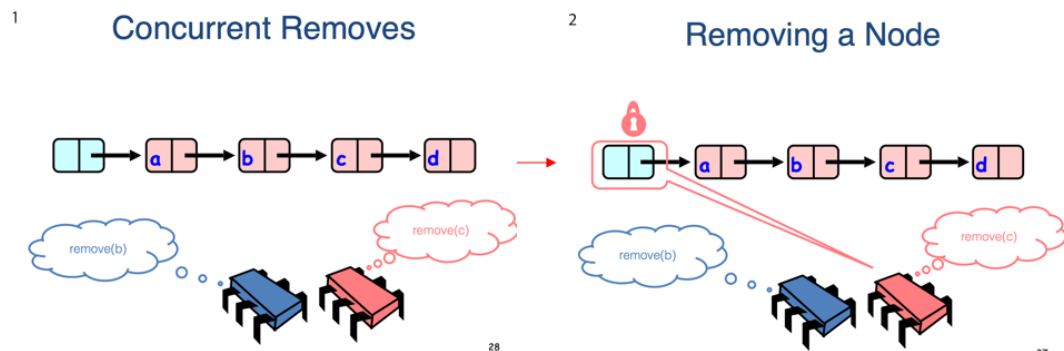
Notice lock is on a struct L

More threads can be locked at once

### • Hand-over-hand locking

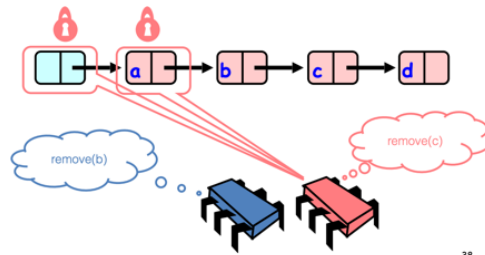
- Idea: instead of having a single lock for the entire list, a lock per node of the list is added; when traversing the list, the list grabs the next node's lock, and releases the current node's lock
- Is a fine-grained-locking
- Holds at most 2 locks at a time

### Example



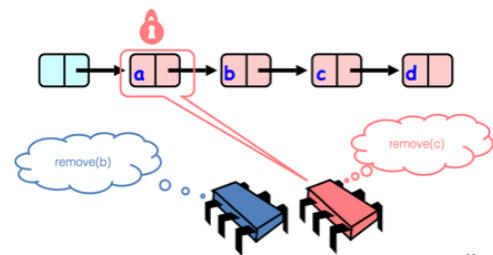
3

## Removing a Node



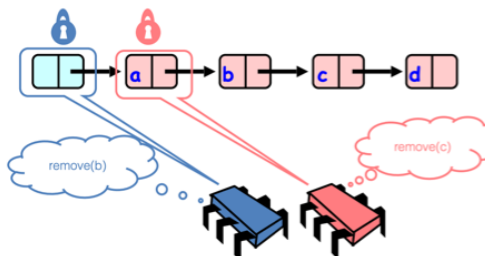
38

## Removing a Node



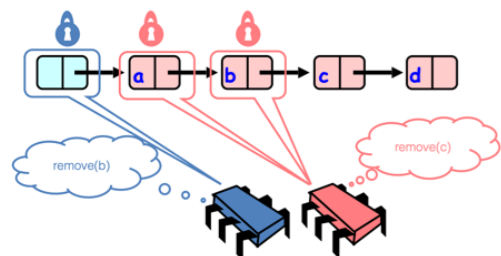
39

## Removing a Node



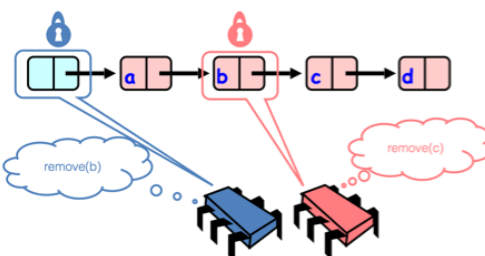
40

## Removing a Node



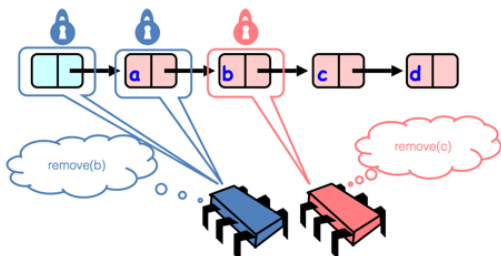
41

## Removing a Node



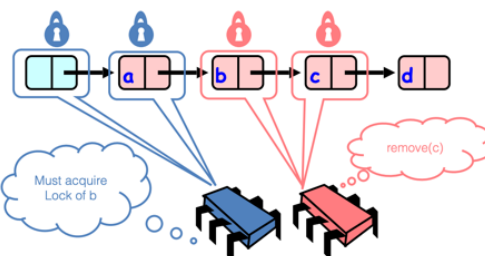
42

## Removing a Node



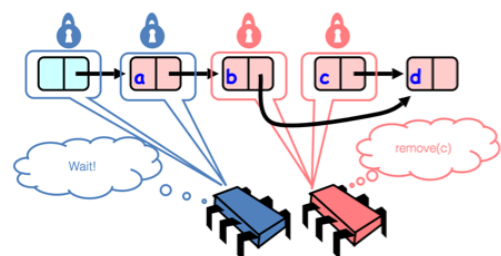
43

## Removing a Node

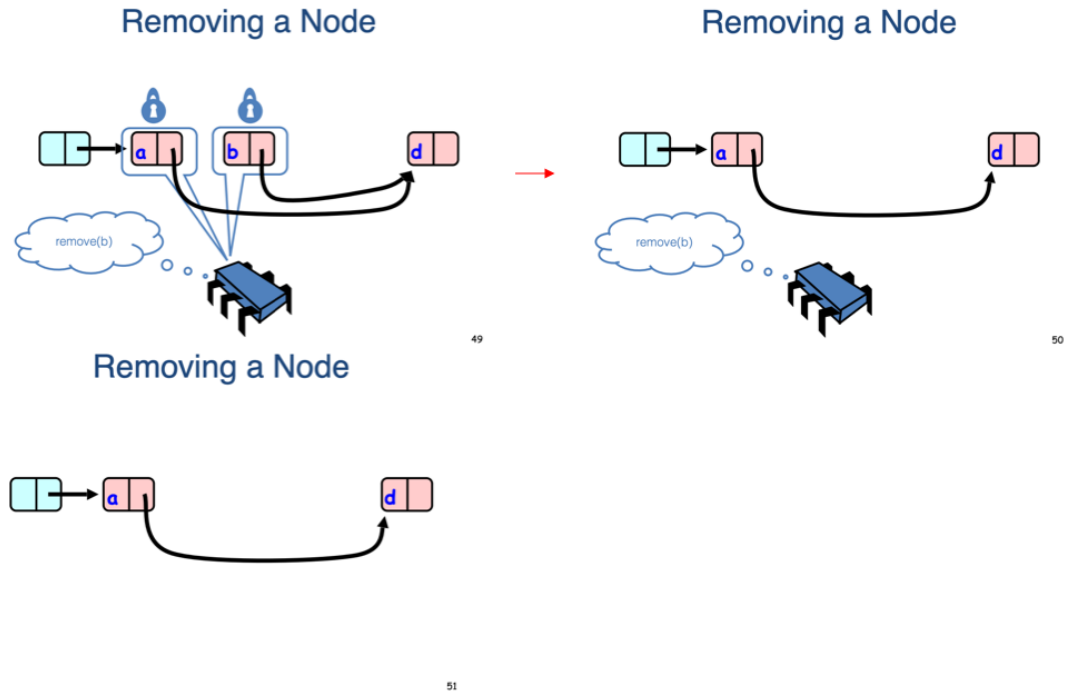


44

## Removing a Node



46



## References

- 1) Tachion, Linked Lists: The Role of Locking, link
- e) Interactive systems emphasizes quick response time, and for non-preemptive scheduling algorithms, the shorter tasks must wait for a process to finish, which means poor response time.

## Notes

### • Preemptive Scheduling Algorithm

- Are designed so that different processes can be executed in the middle of any current process execution.
- Today, all of the modern scheduling algorithms are **preemptive**

### Example

Shortest-Time-To-Completion (STCF) Scheduler

### • Non-preemptive Scheduling Algorithm

- Are designed so that once a process enters the running state, it cannot be preempted (forestalled) until it completes its allotted time

### Example

Shortest Job First (SJF) scheduler

- f) Round Robin uses time slice on each process such that it returns quicker response time than Shortest Time to Completion First scheduling algorithm

**Correct Solution**

SJF is best for minimizing turharound time, but jobs with short cpu bursts can get stuck behind jobs with longer cpu burst

- g) Trap instruction is a non-privileged operation performed in user mode that raises system's privilege level to kernel mode.

**Correct Solution**

A user level process needs to be able to call trap so trap instruction is executed to switch into kernel mode (it's a user-level operation)

**Notes****• Trap**

- Is an exception in a user process <sup>[1]</sup>
- Is an interrupt caused by an exceptional condition (breakpoint, division by zero, invalid memory access) <sup>[2]</sup>
- Is called by user
- Usually results in kernel mode by invoking **trap instruction**<sup>[2]</sup>

**• Trap Instruction**

- when **Trap** or **System call** is invoked, **Trap instruction** simultaneously jumps into the kernel and raise the privilege level to kernel mode

**References**

- 1) StackOverflow, What is the difference between Trap and Interrupt?, link

**2. Notes****• Mutual Exclusion**

- Is a guarentee that is one thread is executing within the critical section, the others will be prevented from doing so.