System Programming
Lab #2

2020-04-01

sp-tas

Lab Assignment #1 – Linker Lab

- Download skeleton code from eTL

- Hand In
  - Upload your files **eTL**
  - A tarball of your implementation (20/20/20/+10 pts for each part)
  - A report (10 pts)

- PLEASE, READ the Hand-out!!!

- Assigned: 3. 25
- Deadline: 4. 8, 11:59:59 PM

Shared library를 통해
Malloc, calloc, realloc, free를 intercept하여
기존의 함수 작업을 하면서
memory tracking도 수행

기존 함수를 호출하면서 구현!

- Lab #2 (4/1) will be Q&A session

(Part 1) Tracing dynamic memory allocation

test1.c

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  a = malloc(32);
  free(malloc(1));
  free(a);
}
```

output

```
stuXXX@spN ~/linklab/part1 $ make run test1
[0001] Memory tracer started.
[0002]            (nil) : malloc( 1024 ) = 0xb87010
[0003]            (nil) : malloc( 32 ) = 0xb87420
[0004]            (nil) : malloc( 1 ) = 0xb87450
[0005]            (nil) : free( 0xb87450 )
[0006]            (nil) : free( 0xb87420 )
[0007]
[0008] Statistics
[0009]   allocated_total      1057
[0010]   allocated_avg        352
[0011]   freed_total          0
[0012]
[0013] Memory tracer stopped.
stuXXX@spN ~/linklab/part1 $
```

(Part 1) Tracing dynamic memory allocation

test1.c

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  a = malloc(32);
  free(malloc(1));
  free(a);
}
```

output

```
stuXXX@spN ~/linklab/part1 $ make run test1
[0001] Memory tracer started.
[0002]            (nil) : malloc( 1024 ) = 0xb87010
[0003]            (nil) : malloc( 32 ) = 0xb87420
[0004]            (nil) : malloc( 1 ) = 0xb87450
[0005]            (nil) : free( 0xb87450 )
[0006]            (nil) : free( 0xb87420 )
[0007]
[0008] Statistics
[0009]   allocated_total      1057
[0010]   allocated_avg        352
[0011]   freed_total          0
[0012]
[0013] Memory tracer stopped.
stuXXX@spN ~/linklab/part1 $
```

Realloc의 경우, realloc size를 전체를 allocated_total에 더함

잘못된 free에 대한 경우는 생각하지 않아도 됨

(Part 2) Tracing unfreed memory

test1.c

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  a = malloc(32);
  free(malloc(1));
  free(a);
}
```

output

```
stuXXX@spN ~/linklab/part2 $ make run test1
[0001] Memory tracer started.
[0002]            (nil) : malloc( 1024 ) = 0x2415060
[0003]            (nil) : malloc( 32 ) = 0x24154c0
[0004]            (nil) : malloc( 1 ) = 0x2415540
[0005]            (nil) : free( 0x2415540 )
[0006]            (nil) : free( 0x24154c0 )
[0007]
[0008] Statistics
[0009]   allocated_total      1057
[0010]   allocated_avg        352
[0011]   freed_total          33
[0012]
[0013] Non-deallocated memory blocks
[0014]   block                size        ref cnt   caller
[0015]   0x2415060            1024        1         ???:0
[0016]
[0017] Memory tracer stopped.
stuXXX@spN ~/linklab/part2 $
```

(Part 2) Tracing unfreed memory

test1.c

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  a = malloc(32);
  free(malloc(1));
  free(a);
}
```

output

```
stuXXX@spN ~/linklab/part2 $ make run test1
[0001] Memory tracer started.
[0002]           (nil) : malloc( 1024 ) = 0x2415060
[0003]           (nil) : malloc( 32 ) = 0x24154c0
[0004]           (nil) : malloc( 1 ) = 0x2415540
[0005]           (nil) : free( 0x2415540 )
[0006]           (nil) : free( 0x24154c0 )
[0007]
[0008] Statistics
[0009]   allocated_total      1057
[0010]   allocated_avg        352
[0011]   freed_total          33
[0012]
[0013] Non-deallocated memory blocks
[0014]   block                size        ref cnt    caller
[0015]   0x2415060            1024        1          ???:0
[0016]
[0017] Memory tracer stopped.
stuXXX@spN ~/linklab/part2 $
```

모두 free가 되었으면 Non-deallocated memory blocks를 출력하지 않음

잘못된 free에 대한 경우는 생각하지 않아도 됨

(Part 3) Pinpointing call locations

test1.c

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  a = malloc(32);
  free(malloc(1));
  free(a);
}
```

```
stuXXX@spN ~/linklab/part3 $ make run test1
[0001] Memory tracer started.
[0002]          main:6  : malloc( 1024 ) = 0x14f0060
[0003]          main:10 : malloc( 32 ) = 0x14f04c0
[0004]          main:1d : malloc( 1 ) = 0x14f0540
[0005]          main:25 : free( 0x14f0540 )
[0006]          main:2d : free( 0x14f04c0 )
[0007]
[0008] Statistics
[0009]   allocated_total      1057
[0010]   allocated_avg        352
[0011]   freed_total          33
[0012]
[0013] Non-deallocated memory blocks
[0014]   block                size        ref cnt    caller
[0015]   0x14f0060            1024        1          main:6
[0016]
[0017] Memory tracer stopped.
stuXXX@spN ~/linklab/part3 $
```

(Part 3) Pinpointing call locations

test1.c

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  a = malloc(32);
  free(malloc(1));
  free(a);
}
```

```
stuXXX@spN ~/linklab/part3 $ make run test1
[0001] Memory tracer started.
[0002]          main:6  : malloc( 1024 ) = 0x14f0060
[0003]          main:10 : malloc( 32 ) = 0x14f04c0
[0004]          main:1d : malloc( 1 ) = 0x14f0540
[0005]          main:25 : free( 0x14f0540 )
[0006]          main:2d : free( 0x14f04c0 )
[0007]
[0008] Statistics
[0009]   allocated_total      1057
[0010]   allocated_avg        352
[0011]   freed_total          33
[0012]
[0013] Non-deallocated memory blocks
[0014]   block              size       ref cnt    caller
[0015]   0x14f0060          1024       1          main:6
[0016]
[0017] Memory tracer stopped.
stuXXX@spN ~/linklab/part3 $
```

Test.c에서 alloc, dealloc 함수는 main에서 호출된다고 가정

Callq instruction의 크기는 실습환경에 맞추어 5바이트라고 가정

Alloc, realloc의 결과로 주소가 겹치는 경우, non-deallocated memory blocks의 caller는 해당 주소에 최초로 alloc한 위치 또는 마지막으로 alloc한 위치 둘 중 하나로 출력

(Bonus) Detect and ignore illegal deallocations

- Detect double- free / illegal free

test4.c – test case for bonus part

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  free(a);
  free(a);
  free((void*)0x1706e90);
}
```

output

```
stuXXX@spN ~/linklab/bonus $ make run test4
[0001] Memory tracer started.
[0002]          main:6  : malloc( 1024 ) = 0x1b30060
[0003]          main:11 : free( 0x1b30060 )
[0004]          main:19 : free( 0x1b30060 )
[0005]              *** DOUBLE_FREE  *** (ignoring)
[0006]          main:23 : free( 0x1706e90 )
[0007]              *** ILLEGAL_FREE *** (ignoring)
[0008]
[0009] Statistics
[0010]   allocated_total      1024
[0011]   allocated_avg        1024
[0012]   freed_total          1024
[0013]
[0014] Memory tracer stopped.
stuXXX@spN ~/linklab/bonus $
```

Free / Realloc 할 때

(Bonus) Detect and ignore illegal deallocations

- Detect double- free / illegal free

test4.c – test case for bonus part

```
#include <stdlib.h>

void main(void) {
  void *a;

  a = malloc(1024);
  free(a);
  free(a);
  free((void*)0x1706e90);
}
```

output

```
stuXXX@spN ~/linklab/bonus $ make run test4
[0001] Memory tracer started.
[0002]          main:6  : malloc( 1024 ) = 0x1b30060
[0003]          main:11 : free( 0x1b30060 )
[0004]          main:19 : free( 0x1b30060 )
[0005]              *** DOUBLE_FREE  *** (ignoring)
[0006]          main:23 : free( 0x1706e90 )
[0007]              *** ILLEGAL_FREE *** (ignoring)
[0008]
[0009] Statistics
[0010]   allocated_total       1024
[0011]   allocated_avg         1024
[0012]   freed_total           1024
[0013]
[0014] Memory tracer stopped.
stuXXX@spN ~/linklab/bonus $
```

realloc의 경우, 잘못된 주소가 들어왔을 경우, free는 무시하고 alloc은 수행 (realloc 입력 주소 값에 NULL)

Double free와 illegal free의 경우 할당 메모리의 시작점 기준으로 할당된 적 있는지 확인

다음 시간에

- 실습 과제2

- 과제 기한 : 4월 8일, 11:59:59 PM