CS6570 Secure Systems Engineering
Assignment 5A

Raghul R (CS16B021), Surya S (CS16B029)

October 18, 2019

Note: Due to large size of the output, typescript is submitted instead of screenshots. View the output using `cat typescript`.

1 Types of bins in ptmalloc2

1. `Fast Bin`: A fast bin is a singly linked list that contains memory chunks of size 16 to 96 bytes. It has **11** bins with each bin storing a list of chunks which are 8 bytes apart in size. Fast bins serve the `malloc()` and `free()` requests for chunk sizes between 16-64 bytes.

2. `Unsorted Bin`: The unsorted bin is a doubly linked circular list that contains memory chunks of size greater than 80 bytes. Any `malloc()` and `free()` requests for memory chunks other than free chunks is first served by unsorted bin before small or large bins.

3. `Small Bin`: Small bins serve all memory chunk requests of less than 512 bytes. It has 62 bins with each bin storing a list of chunks which are 8 bytes apart. It's also a doubly linked circular list.

4. `Large Bin`: Large bins serve all memory chunk requests greater than 512 bytes. It has 63 bins. Unlike small bins or fast bins, chunks belonging to same bins are not same in size. It's also a doubly linked circular list.

2 Experiment and Observations

The test program `t-test1.c` provided was modified to print the sizes of different blocks present in each bin. The experiment originally present in `t-test1.c` was to allocate and free chunks of memory of random sizes up to a fixed maximum size passed as a parameter. The modified test also prints the contents of each bin after all the random allocations and deallocations are completed. The observations are as follows:

1. The number of fast bins is 11 as compared to the usual 10.

2. In the regular bins, the first index corresponds to the unsorted bin, which temporarily contains chunks of all sizes (which do not belong in fast bins) in the order they arrive to the unsorted bin, before they move to the large and small bins appropriately.

3. When the maximum size of chunks is low (around 64), almost all the freed chunks are stored in fast bins.

4. When the maximum size of chunks is intermediate (around 256), an equal number of freed chunks are stored in fast and small bins.

5. When the maximum size of chunks is large (above 512), most freed chunks of size at most 512 are stored in small bins, while freed chunks of size above 512 are stored in large bins.

3 Instructions to execute experiments

1. In the ptmalloc2 folder, replace `t-test1.c` and `Makefile` with one's provided in the submission.

2. Run `make a5`.