Heap 101

陳韋廷

Outline

- Heap & glibc Magic
- Heap Exploitation - Heap Overflow
- Heap Exploitation - Use After Free
- Heap Exploitation - Double Free

Code

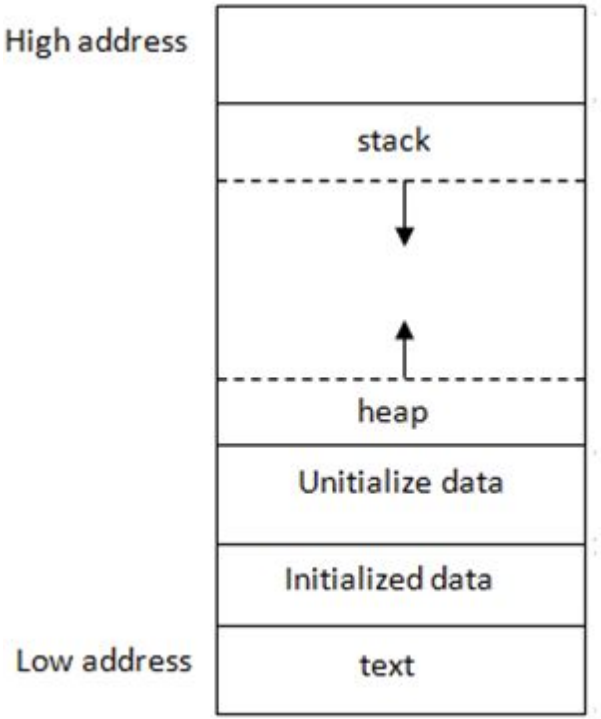
https://github.com/nickchen120235/heap-101

Heap & glibc Magic

- Heap
- malloc() & friends
- Chunk, Arena, Bins, tcache

Heap

- Dynamic allocation
- Grows towards high address
- Allocation by chunks

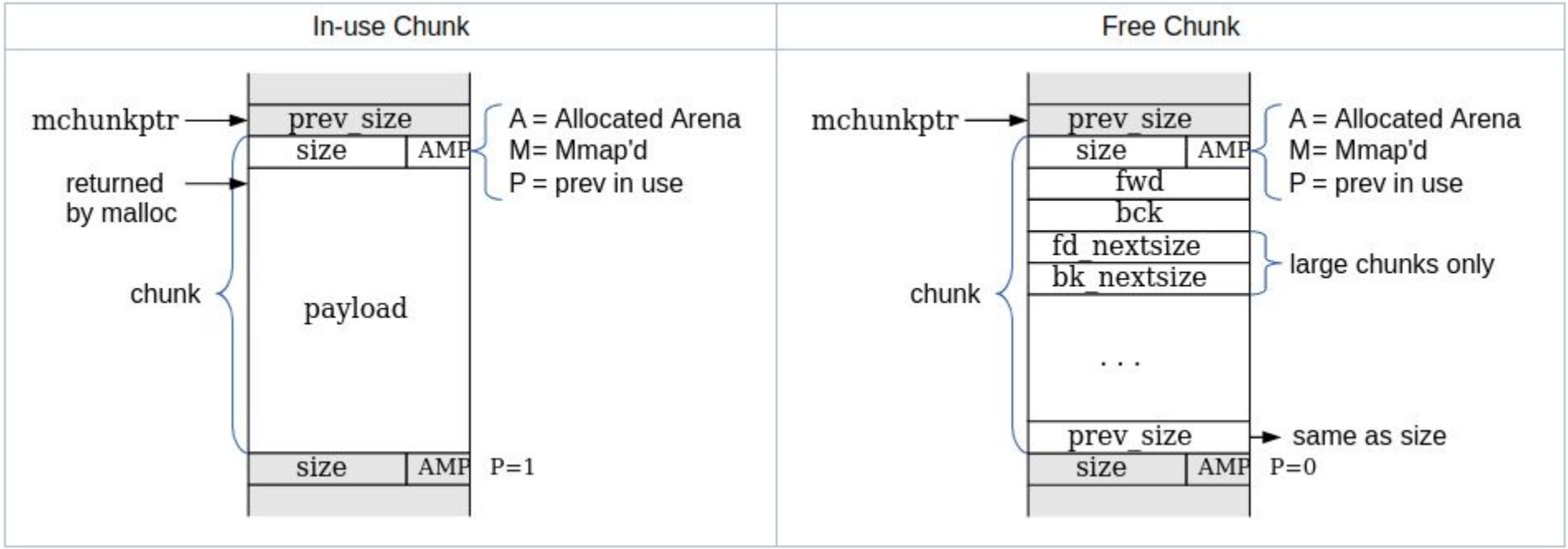


https://courses.engr.illinois.edu/cs225/fa2022/resources/stack-heap/

malloc() & friends

- void* malloc(size_t size): Uninitialized storage
- void* calloc(size_t num, size_t size): Array initialized to zero
- void* realloc(void* ptr, size_t new_size): Reallocate memory
- void free(void* ptr): Deallocate memory

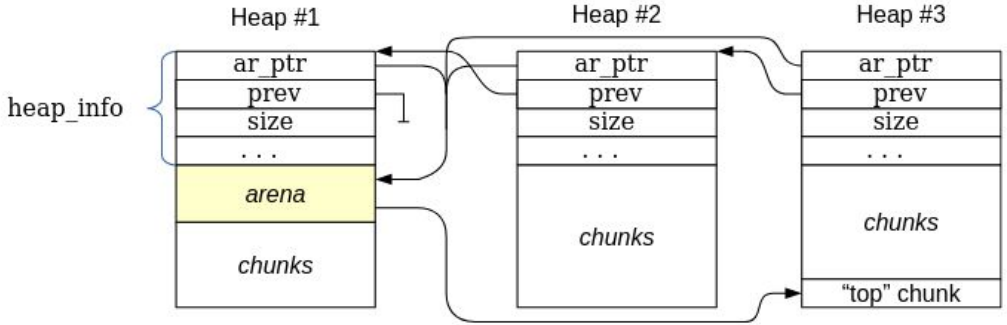
Chunk



https://sourceware.org/glibc/wiki/MallocInternals

Arena

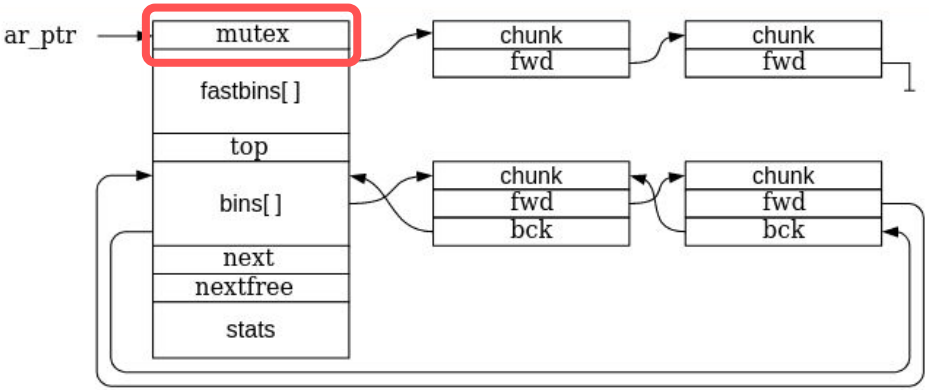
- Main arena: Application’s initial heap
- Additional arenas: mmap()
- Up to 8 * CPU count
- Top: most recently allocated
- mutex-locked



https://sourceware.org/glibc/wiki/MallocInternals

Bins

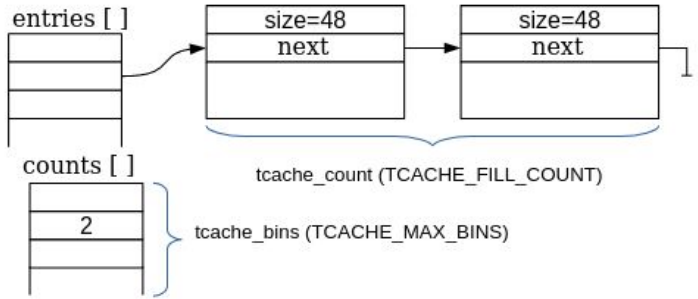
- free()-ed chunks
- Fast
  - Separate bins for each specific sizes
  - Singly-linked list
  - LIFO
- Unsorted
- Small
  - Each chunk is the same size
- Large
  - Best fit
  - Chunks are splitted when needed



https://sourceware.org/glibc/wiki/MallocInternals

Thread Local Cache (tcache)

- Since glibc 2.26
- Singly-linked lists
- Points to payload instead of the chunk header
- Separate bins for each specific sizes
  - Indexed (indirectly) by chunk size
- TCACHE_FILL_COUNT
  - How many chunks can be stored per bin
  - Default: 7
- TCACHE_MAX_BINS
  - How many bins
  - Default: 64



https://sourceware.org/glibc/wiki/MallocInternals

Heap Exploitation

- Heap Overflow
- Use After Free
- fastbin Double Free

Heap Overflow

- Allocation on heap is contiguous

Use After Free

- Pointer to free()-ed memory
- malloc() ➜ free() ➜ malloc()

(fastbin) Double Free

- fastbin only checks the head of the list
- Can be used to launch more complex attacks

Reference

- https://infosecwriteups.com/use-after-free-13544be5a921
- https://github.com/Dvd848/CTFs/blob/master/2021_picoCTF/Cache_Me_Outside.md
- https://firmianay.gitbooks.io/ctf-all-in-one/content/doc/4.14_glibc_tcache.html
- https://sourceware.org/glibc/wiki/MallocInternals
- https://ir0nstone.gitbook.io/notes/types/heap/introduction-to-the-heap
- https://ithelp.ithome.com.tw/articles/10201434