Advanced Cybersecurity Topics

–

Heap Exploitaion

19-20

Exploit Heap Overflow to gain RCE

- Use after free
- Exploit glibc implementation to get:
  - Arbitrary Write
  - EIP Control

Memory Allocations

- **syscall**
  - mmap, munmap
  - brk/sbrk
- **libc**
  - malloc, calloc, realloc, free

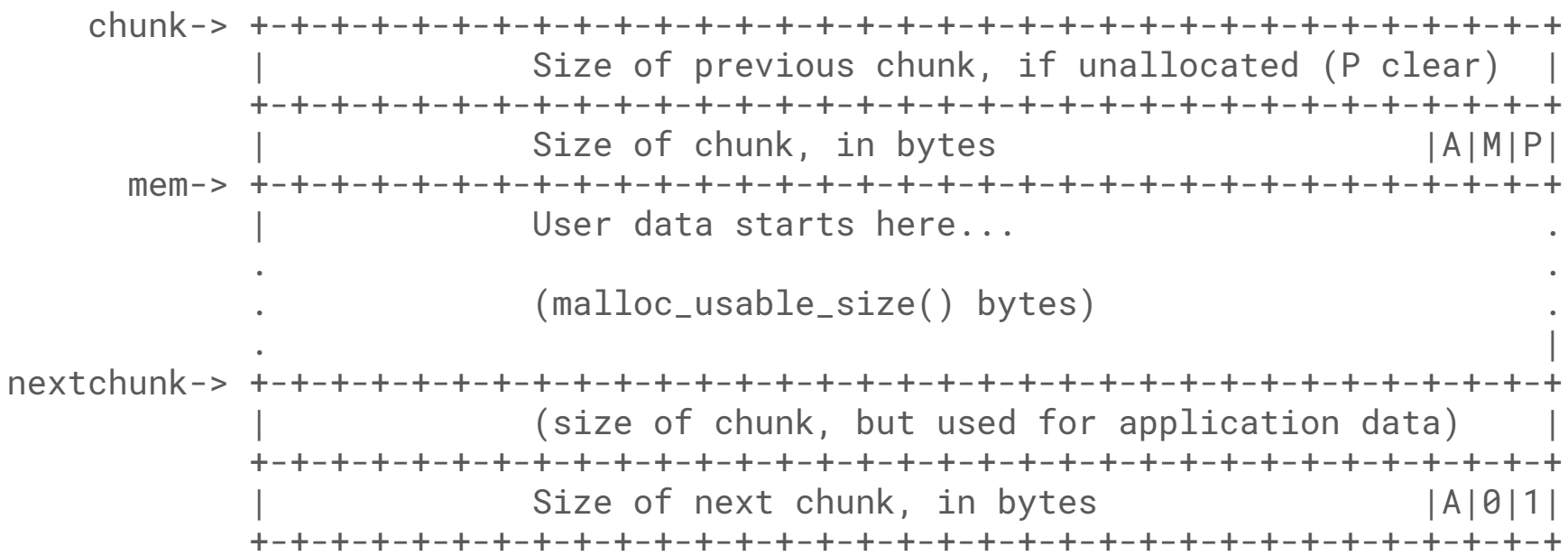
The HEAP Allocators

- **ptmalloc/dlmalloc**
- tcmalloc
- jemalloc
- splittings, fits, coalescing, segregations (free list, storage, non determinism)

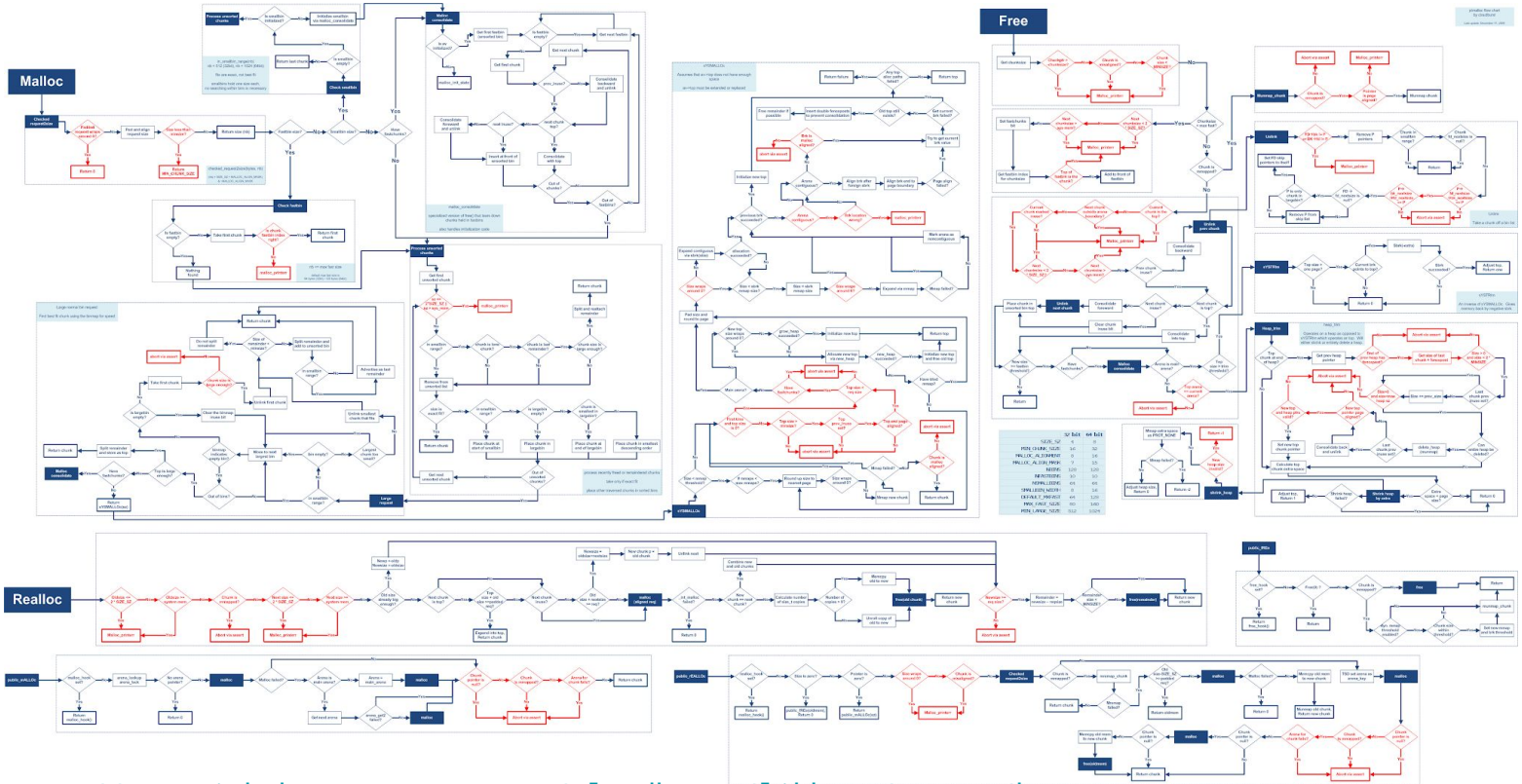
ptmalloc2 (aka the malloc of libc)

- splittings
- fits
- coalescing
- segregations free list
- NO segregations storage
- is deterministic

Best documentation is source code.



Algorithm



https://raw.githubusercontent.com/cloudburst/libheap/master/heap.png

Bins

- t-cache
- Fast bin
- Unsorted bin
- Small bin
- Large bin
- top-chunk

Useful Links

- https://github.com/shellphish/how2heap

- https://sploitfun.wordpress.com/2015/02/10/understanding-glibc-malloc/