Module: Dynamic Allocator Misuse II

Beyond tcache

Robert Wasinger Arizona State University

So far... TCACHE

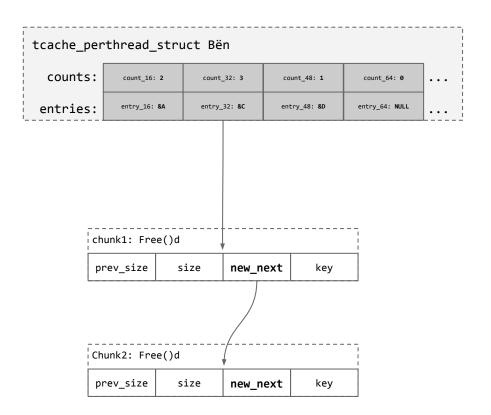
TCACHE

- Bins of constant size up to 1032 bytes
- Caches up to seven freed chunks
- Singly linked list
- Safe-Linking

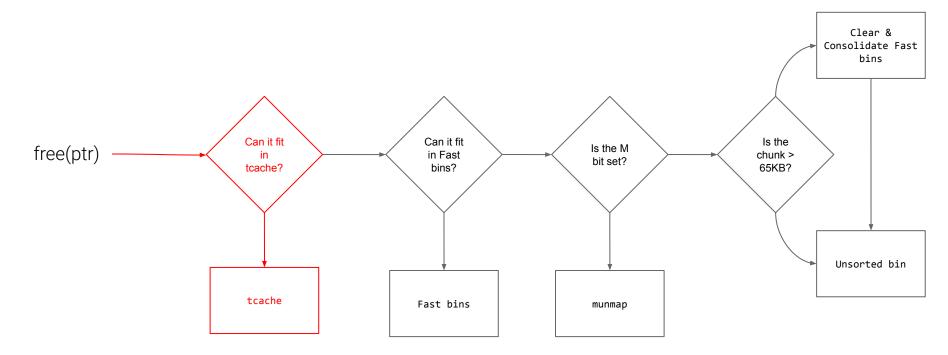
TCACHE Chunk Metadata

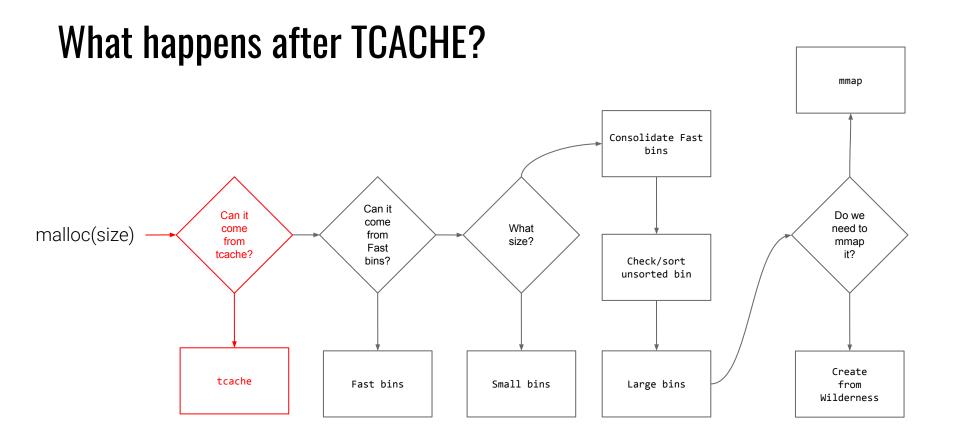
chunk1: Free()d					
prev_size	size			next	key
	А	М	Р		

TCACHE - Singly Linked List



What happens after TCACHE?





More metadata

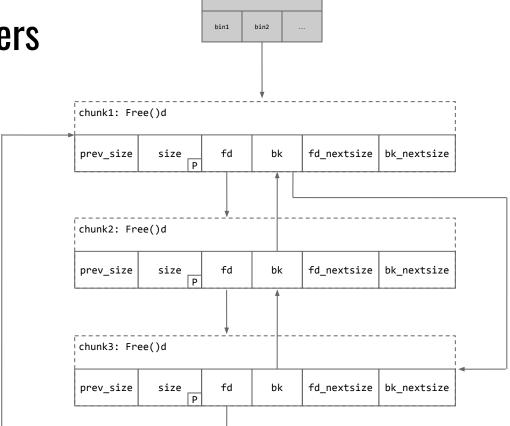
chunk1: Free()d					
prev_size	size	fd	bk	fd_nextsize	bk_nextsize

More lists

Singly Linked List							
	Fast bins		tcache				
entry_16	entry_24		entry_16	entry_32			

Doubly Linked Lists								
		small bins		large bins				
unsorted bin	bin1	bin2		bin1	bin2			

More pointers



small bins

Consolidation

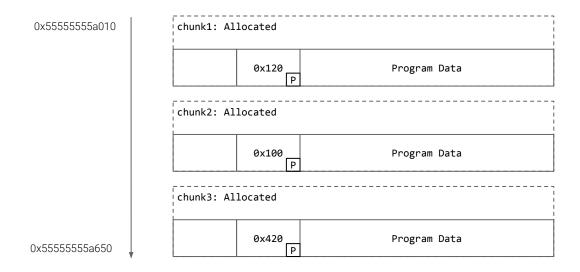
- Consolidation is why a doubly linked list is necessary
- Combines two neighboring chunks
- This can occur:
 - When a chunk is freed
 - When a chunk is malloc'd.
- Consolidation requires the removal of an entry after merging

Consolidation

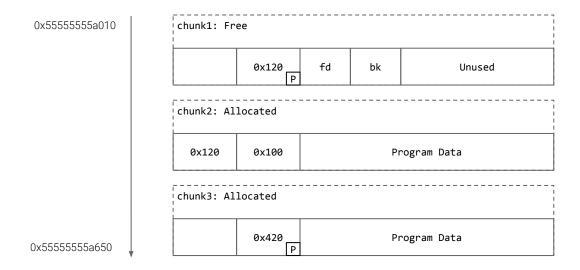
- Consolidation occurs forward and backward!
- The P bit must be cleared for a chunk to consolidate

chunk1: Free()d				chunk2: Free()d							
prev_size	size P	fd	bk	fd_nextsize	bk_nextsize	prev_size	size P	fd	bk	fd_nextsize	bk_nextsize

Initial state



free(0x5555555a028)



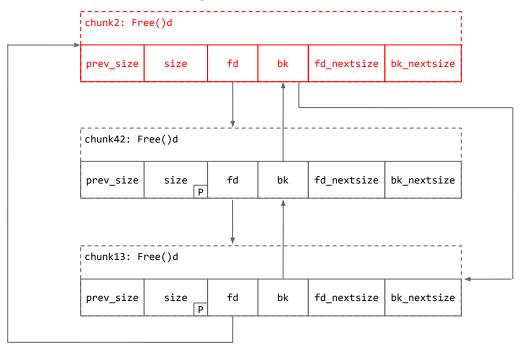
free(0x5555555a028)

0x55555555a010	chunk1: Fr	chunk1: Free							
		0x120 P	fd	bk	Unused				
	chunk2: Al	chunk2: Allocated							
	0x120	0x100	fd	bk	Unused				
	chunk3: Al	chunk3: Allocated							
0x55555555650	0x100	0x420		Pr	rogram Data				

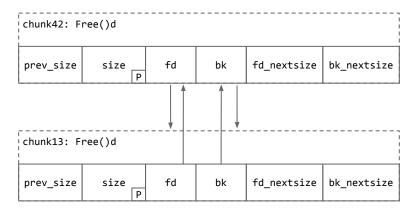
free(0x5555555a148)

0x555555555a010	chunk1: Fr	chunk1: Free						
		0x220 P	fd	bk	Unused			
		Unused						
	chunk3: Al	located						
0x55555555650	0x220	0x420		Pi	rogram Data			

Consolidation - Unlinking



Consolidation - Unlinking



Consolidation - Unlinking verification

```
/* Take a chunk off a bin list. */
static void unlink chunk (mstate av, mchunkptr p) {
if (chunksize (p) != prev size (next chunk (p)))
    malloc printerr ("corrupted size vs. prev size");
 mchunkptr fd = p->fd;
 mchunkptr bk = p->bk;
 if ( builtin expect (fd->bk != p || bk->fd != p, 0))
    malloc printerr ("corrupted double-linked list");
 fd \rightarrow bk = bk;
 bk \rightarrow fd = fd:
```