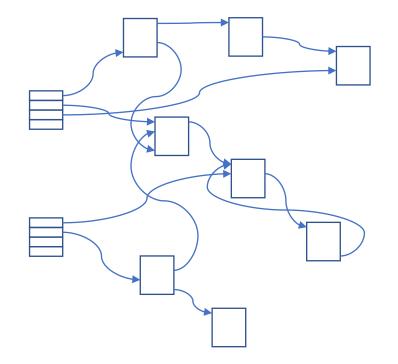
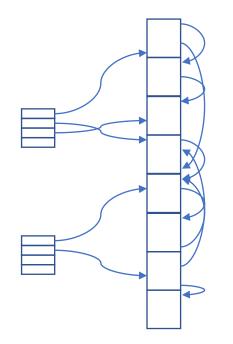
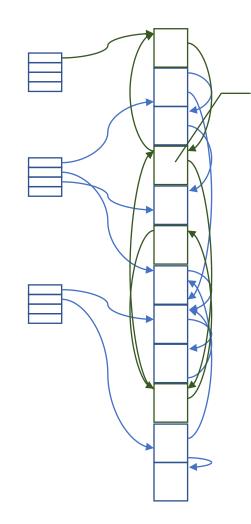
### Towards a Safe, High-Performance Heap Allocator

Lessons from CHERIfying snmalloc (so far)

David Chisnall

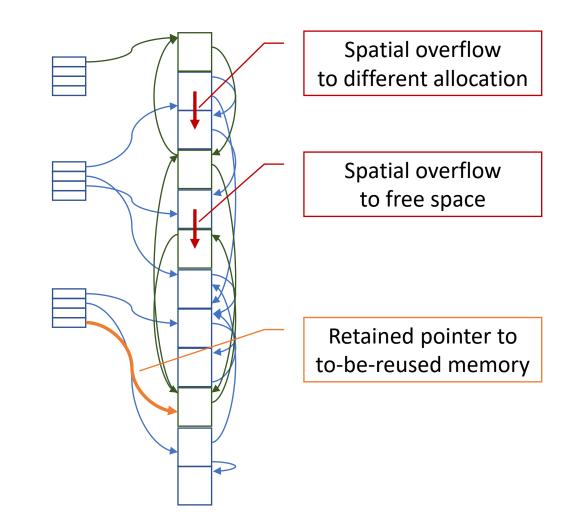




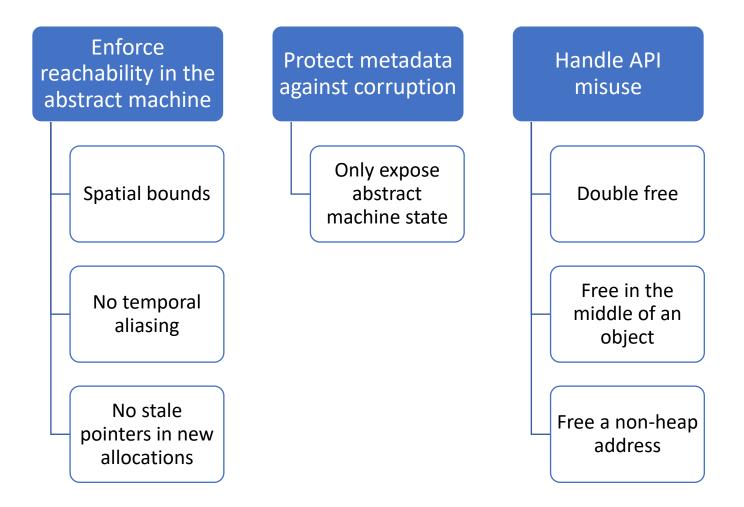


Free regions for reuse must be tracked by allocator

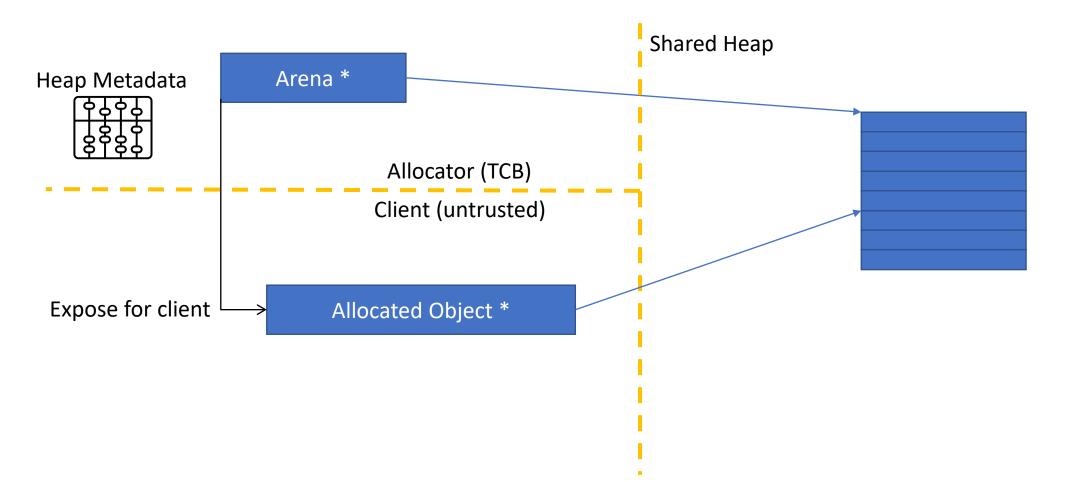
#### Less-than-full abstraction



#### Towards full abstraction for the heap



#### Heap allocator is a core part of the TCB



DEAAGCEGOS 3J CONTRACTOR DEPSION OF E96 OUARES96D:D :D E92E =65FCD 56D46:565 7C8> =6C:D:78C W=8C:DA=:<6X AC:>2860] 99:D :D DEAAGCEGO 3J (100 PERS) (100 PE DUGDD], g., h.,a\_. p >@C6 C64621256DECF4E2CC2?86>65C? DEC6AD:CC9??6D 42? J:6=5 :7D:89ED 6? AC:>2E6D 42? J:6=5 :7D:89ED 6? AC:>2E6D 42? J:6=5 :7D:89ED 6? AC:SEG 255 ACG6255 C6062C49 DFAAGCE65 3J DFFAAGCE65 3J DFFAAGCE 40?ECC 65 DEC ?8D] 2?5C2:?70C6DED 0740ECC 97 65FCD[ 296 2524:70C5D 275 E96 AC6D6746 07 E96 DEC6AD:CO::: DEC 40.1 CO::: DEC 40. C. 2?46DEC2= =6 FCD 2C6 E90F89E E0 92G6 @C:8:?E96:CWO'e\_>J2X[ p?E2C4E:42 WOg\_-'b\_>J2X[ 2?5 x?5:2 WOg\_-h\_>J2X] a66? :DE=2865 D:?46 :E 3CEK6 2H2J 7CB> and p7C:42 #6 A0CE #7 and p7C:42 #7 a E96 r92??6=[ 2 566A 492??6=@36EH66? A@DD6D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 2C@F?5 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 4C@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36EE66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 AC@DD65 E96 [@K2>3:EF6 r92??6=[ 2 566A 492??6=#36E66 A@D66D2E65 :? p7C:42 ea E@ ed >J2[ E96J H@F=5 9266 ea E@ ed >J2[ E0 E E@ ed >J2[ E0 E E@ ed >J2[ E0 E@ ed >J2[ E0 E@ ed >J2] E@ ed =J2[ E0 E@ ed =J2[ E0 E@ ed =J2] E@ ed =J2[ E0 E@ ed =J2[ E0 E@ ed =J2] E@ ed =J2[ E0 E@ ed =J2[ Ed =J2] E@ ed =J2[ E 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8DE96p7C:42 2?5 |25282D42C H:E9 2 >:?:>F> H:5E9 @7 23@FE de\_ <> Wbd\_ >: 5:G6CD:EJ \$66 2=D@i \$F37@DD:= =6>FC p 8:2?E =6>FC 92?8D C>D 2C6 D=:89E=J =0?86C E92? E9640?EC0C0> 2 EC66 =:>3 3J 2== 70FC 766E =:<6 2 D=0H\>0G:?8 D=0E9] \$96 E2:= :D D90CE[ 275 E96 2C>D 266 D=:89E-J =0 100 CE 200 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ {6>FCDJ2X=68D] p =:76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X=68D] p =:76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X=68D] p =:76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X=68D] p =:76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 68D] p =:76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? EH@ E9@FD2?5 J62CD 28@ [6>FCDJ2X = 76 C6DE@C2E:@? @7 q232<@E:2 C25@7:=2:[ 2 D=@E9 =6>FC E92E 3642>6 6IE:?4E =6DD E92? E#@C2E:# b . %96:C 5:G6CD:EJ :? 3@E986?6E:492G6 252AE65 E@ 7:== >2?J @A6? 64@=@8:42= ?:496D D:?46 >2<:?8 E96:C H2J E@ [25282D42C], h. b. %96:C 5:66CD:EJ :? 3@E9 COJD 2?5 2AGD 70F?5 6=D6H96C6 :? E96 H@C=5], a. #2?8:?DA643692G:@C 2?5 >@CA90=@8J W0FEH2C5 2AA62C2?46X C:G2=D E92E 07 E96 >0?<GJD 2?5 2AGD 70F?5 6=D6H96C6 :? E06 H@C=5]</p> CCSVD D>2==6DE AC:>2E6[,ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@> E96 b\_ 8 W`]` @KX [252>6 gree by W@FEH2C5 2AA62C2?46X C:62=D E92E @7 E96 >@?<6JD 225 2A0D 7@?25 6=D6H96C6 :? 69 H C3 226 [ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@> E96 b\_ 8 W`]` @KX [252>6 gree by >@FD6 =65PC[ E96 H@C=5VD D>2==6DE AC:>2E6 [ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@> E96 b\_ 8 W`]` @KX [252>6 gree by >@FD6 =65PC[ E96 H@C=5VD D>2==6DE AC:>2E6 [ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@> E96 b\_ 8 W`]` @KX [252>6 gree by >@FD6 =65PC[ E96 H@C=5VD D>2==6DE AC:>2E6 [ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@> E96 b\_ 8 W`]` @KX [252>6 gree by >@FD6 =65PC[ E96 H@C=5VD D>2==6DE AC:>2E6 [ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@> E96 b\_ 8 W`]` @KX [252>6 gree by >@FD6 =65PC[ E96 H@C=5VD D>2==6DE AC:>2E6 [ba. E@ E96 C646?E=J 6IE:?4E `e\_- 8 :? D:K6 7C@ =24 < 2?J D92C65 EC2:ED E92E >2<6 E96 DE2?5 @FE 7C@> 4@>A=61:EJ (?5 f:: 0 for 200 275 f **17=J 3J C6467E @C DF37@DD:= C6>2:?D[ E96J H6C6 >@56C? =6>FC E:= C646?E=J[ 8:2?E =6>FCD 6I:DE65 @? [25282D42C] }@H c6Ac6D67E5 @? E96C E922 @C DF37@DD:= C6>2:?D[ E96J H6C6 >@56C? =6>FC E:= C646?E=J[ 8:2?E =6>FCD 6I:DE65 @? [25282D42C] }@H c6Ac6D67E5 ? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 < 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 < 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 < 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 & 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 & 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 & 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 & 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96C 2528E2E B6C6 & 7000 E92E B6C6 @? 46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 6G@=G65 :? :DE=2E:@?] \$@>6 @P E96:C 2528E2E @? D B6C6 F? =:C 10 0 C6=2F:C 10 0 C6=2** -2C86C E92? E96 GIE22E W=:G:?8X 7@C>D[ D@>6 H6:89:?8 2D E92E H6C6 @?46 A2CE @7 E96 C:49 =6>FC 5:G6CD:EJ E92E 92D 66@=G65 :? :D@=2E:02] \$0>6 07 E96:C 252AE2E TO H6C6 E94 H6C6 DE>6 86:89:28 20 0000 0667 0000 C +:0: 00-00:0001.0', p+ 1 38 

Threat		Pre-CHER			Canary free obj	ects and occasional tests of livene
Spatial separation		General	Canaries	, ,		
Information disclosure						
Temporal aliasing						
Metadata	Out-of-band					
access or corruption	In-band					
Incorrect fre	20					
Randomized defenses		S	Dete	rministic	w/ issues	Solved (!?)

Threat		Pre-CHER			Canary free obje	ects and occasional	tests of liveness
Spatial sepa	ration	General	Canaries		Look up alloca	ator metadata for s	ource & dest!
		memcpy	Checked				
Information	disclosure						
Temporal al	iasing						
Metadata	Out-of-band						
access or corruption	In-band						
Incorrect fre	e						
Rando	omized defense	es in the second s	Dete	rministic	w/ issues	Solved (!	?)

Threat		Pre-CHER	RI		Canary fr
Spatial sepa	ration	General	Canaries	í	Look u
		memcpy	Checked	·	
Information	disclosure	0 on allo	c (optional)		
Temporal ali	iasing				
Metadata	Out-of-band				
access or					
corruption	In-band				
Incorrect fre	סנ				
Rando	omized defense	S	Dete	erministic	w/ issues

Solved (!?)

**Deterministic w/ issues** 

	Pre-CHERI		
ration	General	Canaries	
	memcpy	Checked	ĺ
disclosure	0 on alloc	(optional)	
asing	Randomize queues		
Out-of-band			
In-band			
е			
	disclosure asing Out-of-band In-band	ration General General memcpy disclosure O on alloc asing Queues Randomize Queues In-band In-band	ration General Canaries memcpy Checked O on alloc Uptional asing Randomized free queues Out-of-band Randomized Iocation & guard pees

**Randomized defenses** 

Canary free objects and occasional tests of liveness

Look up allocator metadata for source & dest!

Opt-in zero when allocating

Randomization to frustrate attacker's attempts to locate objects of interest

Threat		Pre-CHERI		
Spatial sepa	ration	General	Canaries	/
		memcpy	Checked	/
Information	disclosure	0 on alloc	(optional)	
Temporal al	iasing	Randomized free queues		
Metadata	Out-of-band	Randomized location & guard pages		
access or corruption	In-band	Pointer obfuscation & lightweight MAC		
Incorrect fre	e	个 & (opt-in) check of ptr to object start		

Canary free objects and occasional tests of liveness

Look up allocator metadata for source & dest!

Opt-in zero when allocating

Randomization to frustrate attacker's attempts to locate objects of interest

Optional "encrypt and MAC" on in-band metadata: minimizes disclosure and detects tampering (whp)

"Same object twice" DF, not "temporally aliased"

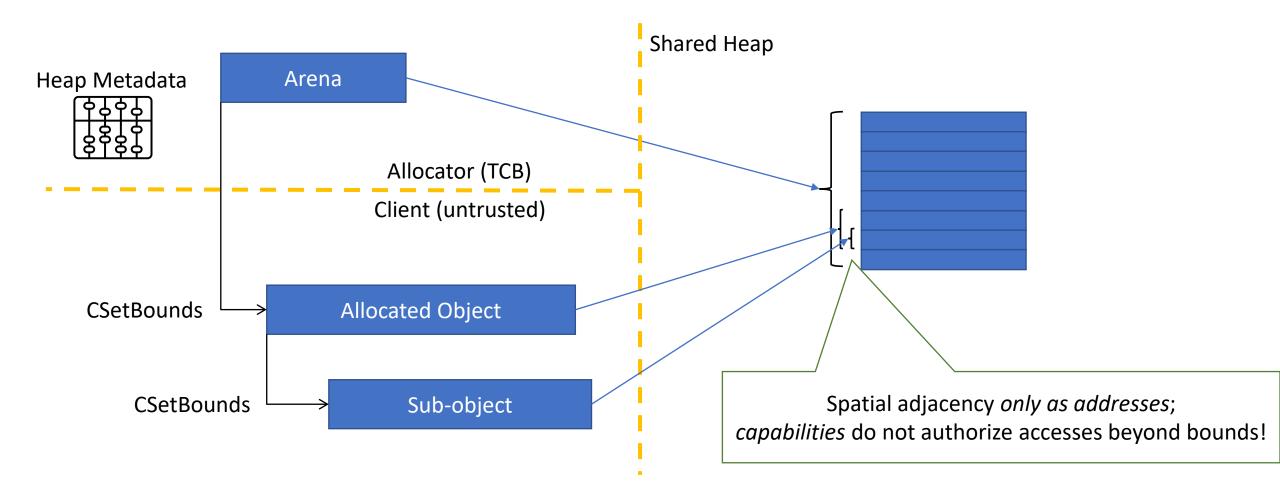
**Randomized defenses** 

Deterministic w/ issues

Solved (!?)

## Enter CHERI

#### CHERI capabilities capture provenance

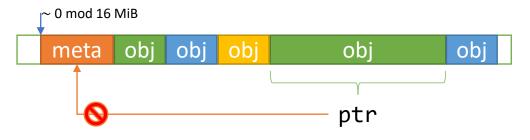


#### What about free()?

Per-object headers?

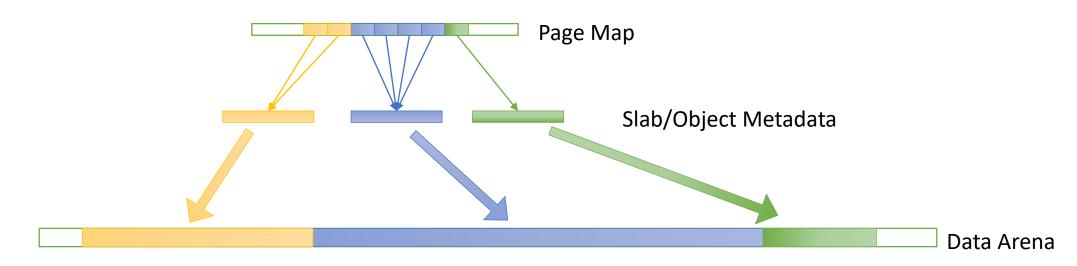


Per-segment headers?



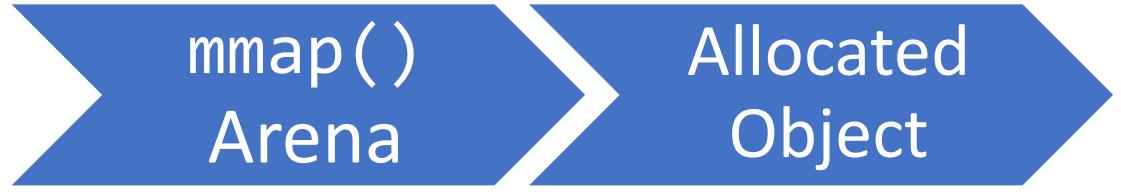
- Bounding in malloc() means free() can't use argument as pointer!
  - Need to reach metadata via allocator-private state (global/TLS/handle)





- snmalloc's central internal data structure is its "Page Map" (VA / 16KiB) → Per-Slab or Per-large-object Metadata
- Convenient place to stash widely-bounded pointers

#### Don't stare into the **void**\*

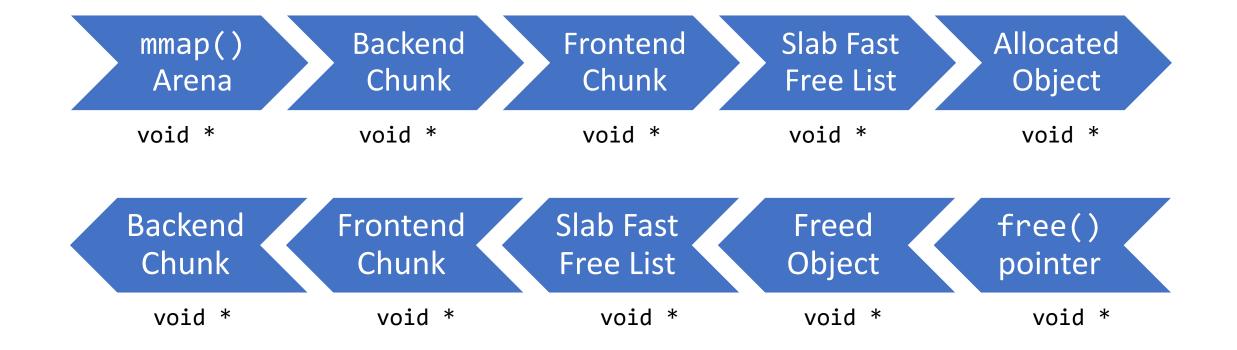


void \*

void \*



#### Don't stare into the void\*



#### Don't stare into the **void**\*

CapPtr<T,B> aka B<T>: T\* with static bound annotation B (Arena > Chunk > Alloc > Wild)



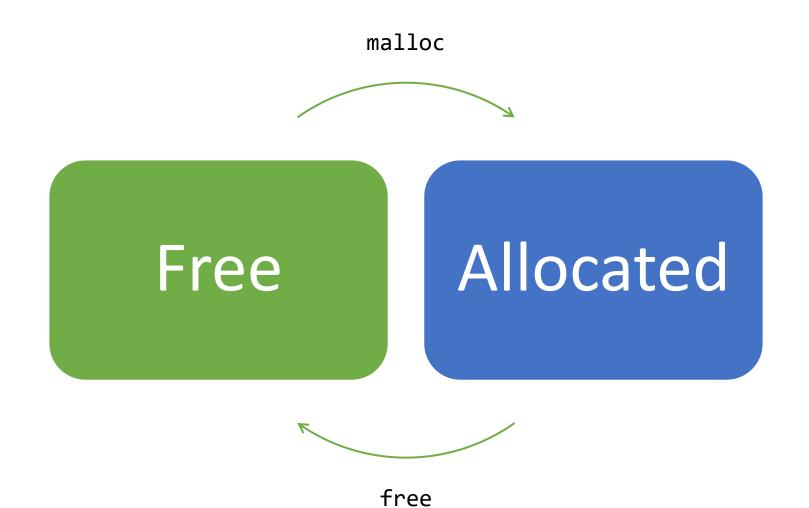
CapPtr<T, BOut> capptr\_bound(CapPtr<U, BIn>, size\_t); // BOut ≤ BIn void\* capptr\_reveal(Alloc<void>);

#### Initial CHERIfication of snmalloc

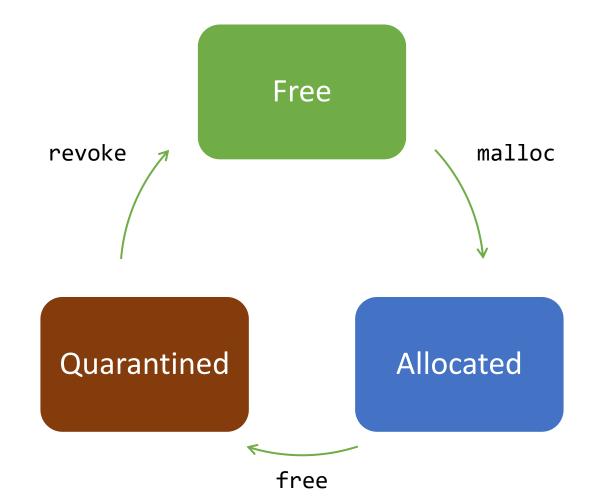
Threat	Threat		Pre-CHERI			C	CHERI spatial bounds do their thing!		
Spatial sepa	Spatial separation		Canaries	Set bounds				R:	
		memcpy	Checked		_		Still just randomized defenses		
Temporal ali	iasing	Randomized free		÷			,,		
		queues					CapPtr eases auditing		
Information	Information disclosure		0 on alloc (optional)			Cli	Clients not linked to snmalloc glo		
N de te de te	Out-of-band	Randomized location		Capability			but arena caps can still be leaked		
Metadata access or		& guard p	pages	reachability		Canal	Capability bits are precious; can't obfuscat	scate	
corruption	In-band	Pointer obfuscation		Seal* & MAC			but can <i>seal</i> (not yet done) and can still N		
			& lightweight MAC						
Incorrect free		↑ & (opt-in) check of		个 &					
	ptr		ject start	$\leftarrow$ 's check					
Rando	Randomized defenses			rministic w/ iss	sues		Solved (!?)		

### Cornucopia, Take 2 CHERI heap temporal safety

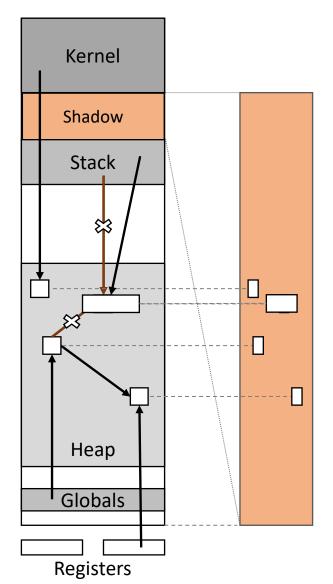
#### Address-space quarantine



#### Address-space quarantine

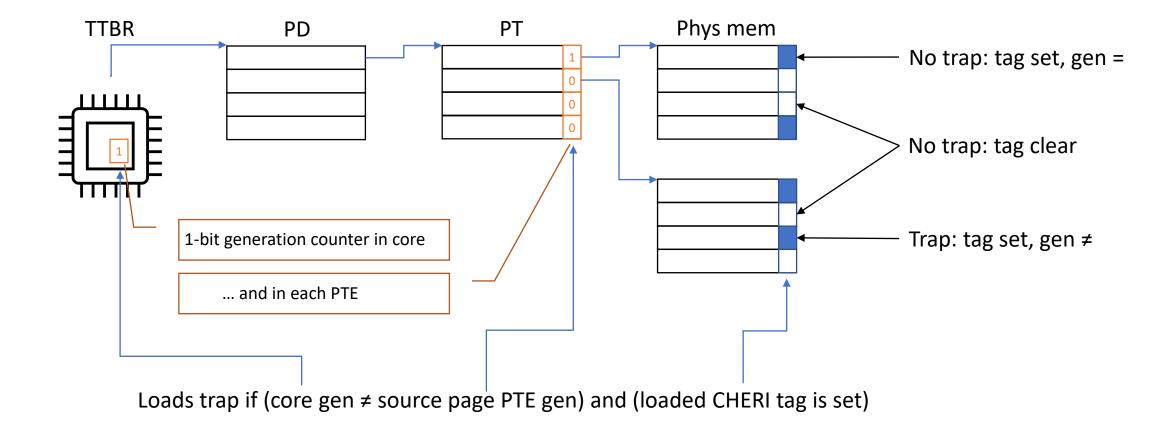


#### Cornucopia quarantine & revocation

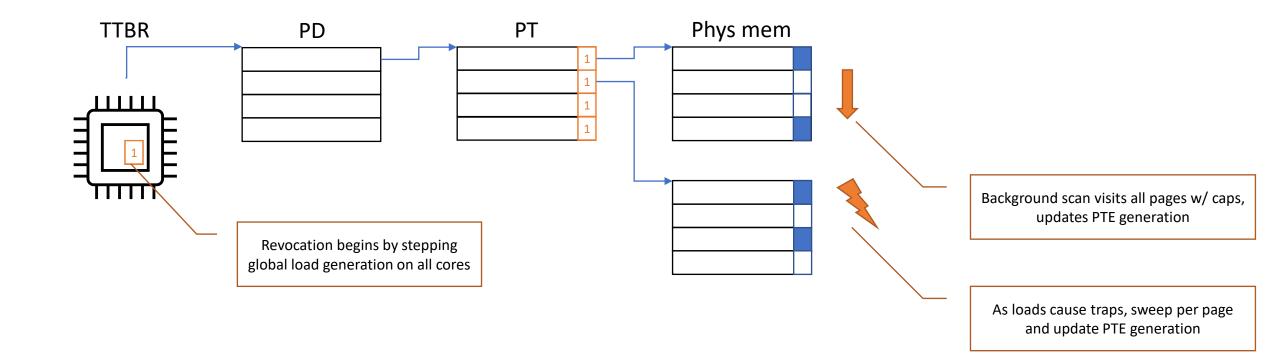


- Application free()-s object, might retain references.
- Express quarantine by painting *shadow* bitmap
  - Live and free objects have 0 shadow bits.
- Eventually, ask kernel to revoke stale caps
  - Sweep AS & remove caps w/ base address shadow bit set
- After revocation, stale caps gone,
  - Now safe to clear shadow bits, &
  - re-issue *unaliased* address space!

### New architecture Per-page capability load generations



#### Revoking with capability load generations



### Threat assessment w/ CHERI & cornucopia

Threat	Threat		CHERI+Revocation		
Spatial separation		Set bounds	$\leftarrow$	<u> </u>	Address space quarantine & revocation eliminates dangling pointers
Temporal al	Temporal aliasing		Quarantine & revocation		Zeroing post quarantine implies 0 at alloc, but leaves quarantine full of junk.
Information	Information disclosure		0 on de-quarantine	l	but leaves quarantine fun of junk.
Metadata	Out-of-band	Capability reachability	$\leftarrow$		Quarantine tracked out-of-band;
access or corruption	In-band	Seal* & MAC	Reuse only after revocation		Metadata in-band <i>only once unaliased</i> At entry to quarantine:
Incorrect fre	Incorrect free		Interlocks w/ quarantine	· [	pointer validation & atomic claim of AS
Rando	omized defense	S	Deterministic w/ issue	es	Solved (!?)

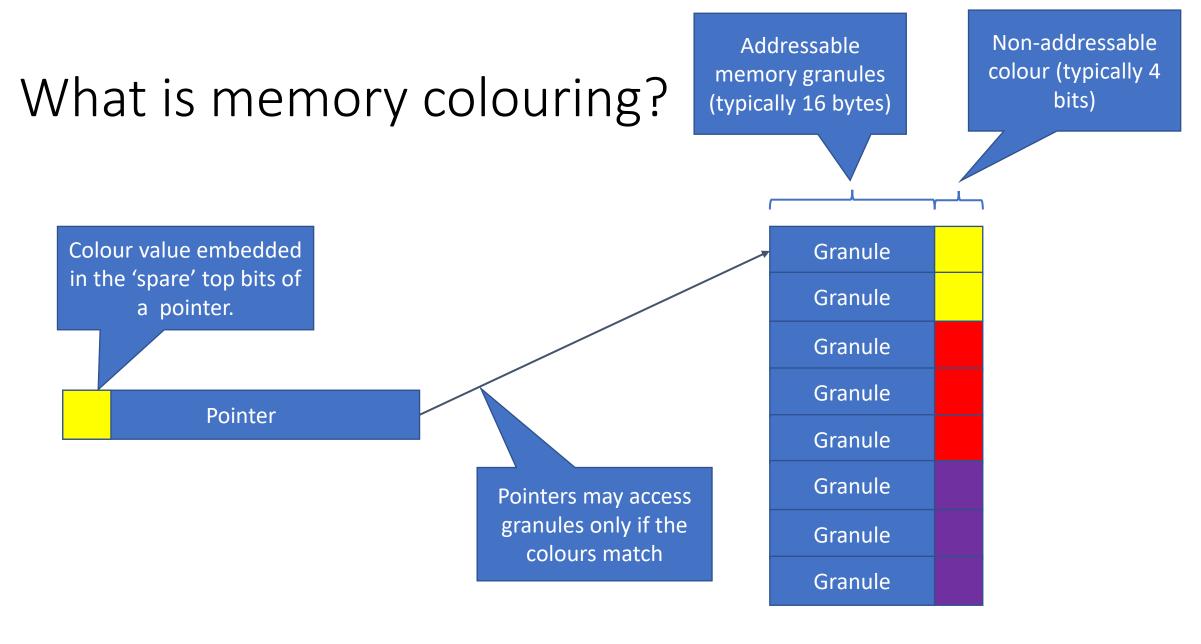
#### Very early revocation benchmarks

- An unoptimized implementation, no statistical power; do not quote!
- SPEC CPU2006 on Morello w/ load generations

Wall time	gobmk 13x13	astar BigLakes2048	omnetpp	xalancbmk
Single core	0.69%	1.7%	24%	23%
Revocation offload (SMP)	0.44%	1.1%	12%	20%

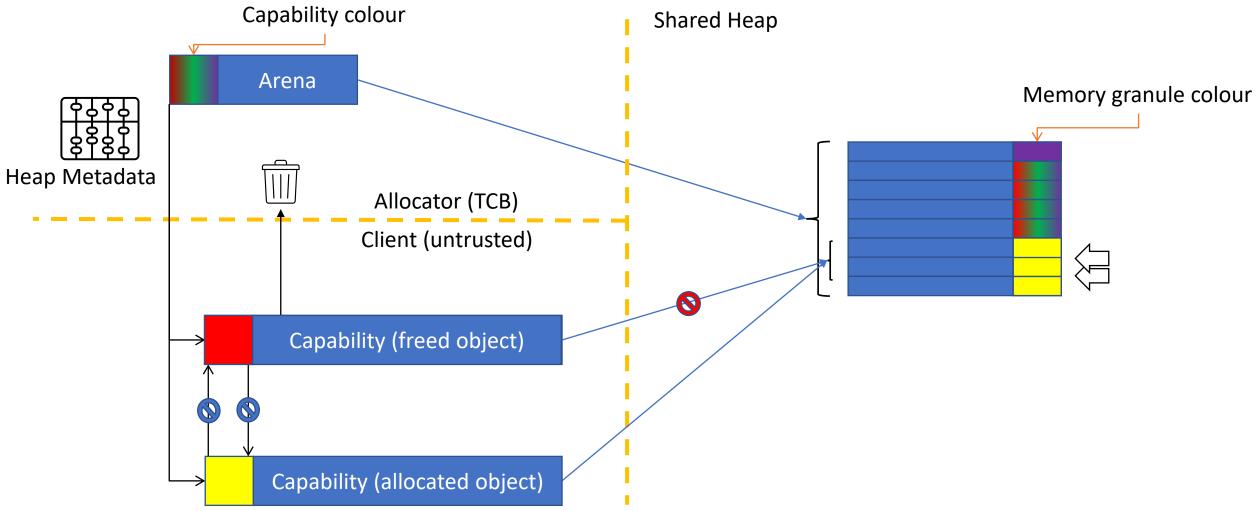
#### CHERI+MTE

#### Memory colouring for faster and better temporal safety

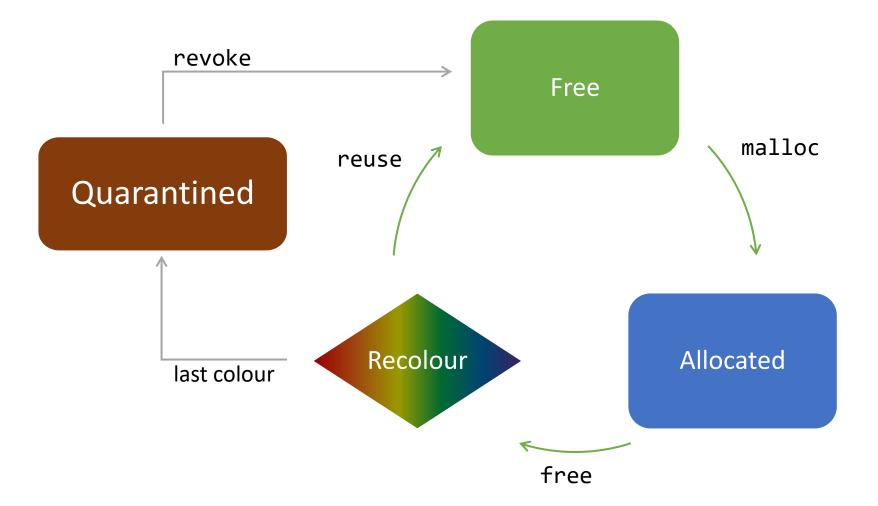


Main memory

### Beyond Morello: non-orthogonal CHERI+MTE in heaps



#### Colouring & Revocation



#### snmalloc CHERI+MTE threat assessment

Threat		CHERI+	Revocation	CHERI+Rev+MTE			
Spatial separation		Set bou	inds	÷		Recolouring reduces quarantine pressure	
Temporal aliasing		Quaran	tine & revocation	Recolour & ←		Zero-on-free combines w/ recolou clears stale caps, & is safe from c	
Information	Information disclosure		-quarantine	0 on free		clears stale caps, & is sale from c	
Metadata	Out-of-band	Capabil	ity reachability	$\leftarrow$		Quarantine/free state in-band ag	
access or corruption In-	In-band	Reuse o revocat	only after ion	Reuse only after recolouring	/	Similar atomic sequence	
Incorrect free		Interlocks w/ quarantine		Interlocks w/ recolouring	/		
Randomized defenses			Deterministic w/ issues			Solved (!?)	

#### snmalloc with CHERI summary

Threat		Pre-CHER	ł	CHERI	CHERI+Revoc	ation	CHERI+Rev+MTE
Spatial sepa	Spatial separation		General Canaries		$\leftarrow$		$\leftarrow$
		memcpy	Checked				
Temporal aliasing		Randomized free queues		÷	Quarantine & revocation		Recolour & ←
Information	Information disclosure		0 on alloc (optional)		0 on de-quarantine		0 on free
Metadata	Out-of-band	Randomized location & guard pages		Capability reachability	$\leftarrow$		÷
access or corruption	In-band	Pointer obfuscation & MAC		Seal* & MAC	Reuse only after revocation		Reuse only after recolouring
Incorrect free		↑ & (opt-in) check of ptr to object start		↑ & ←'s check	Interlocks w/ quarantine		Interlocks w/ recolouring
Randomized defenses			Deterministic w/ issues			Se	olved (!?)

#### Current state of CheriBSD temporal safety

- snmalloc has baseline CHERI support (no quarantine)
  - Composes with "mrs wrapper" library providing a form of quarantine
  - Active work towards *integrated* quarantine
- Available for experimentation now, from source:
  - Kernel, userspace support, mrs, & integrated dlmalloc
- Next CheriBSD release (October) should have initial support:
  - Baseline support in userspace, bypassed on default non-Cornucopia kernels
  - 2<sup>nd</sup>, Cornucopia-enabled kernel as boot option
  - LD\_PRELOAD malloc(s) and mrs wrapper as optional packages

#### One more thing...

What's the smallest variety of CHERI? MSRC / By Saar Amar / September 5, 2022

The Portmeirion project is a collaboration between Microsoft Research Cambridge, Microsoft Security Response Center, and Azure Silicon Engineering & Solutions. Over the past year, we have been exploring how to scale the key ideas from CHERI down to tiny cores on the scale of the cheapest microcontrollers. These cores are very different from the desktop and server-class processors that have been the focus of the Morello project.

Microcontrollers are still typically in-order systems with short pipelines and tens to hundreds of kilobytes of local SRAM. In contrast, systems such as Morello have wide and deep pipelines, perform out-of-order execution, and have gigabytes to terabytes of DRAM hidden behind layers of caches and a memory management unit with multiple levels of page tables. There are billions of microcontrollers in the world and they are increasingly likely to be connected to the Internet. The lack of virtual memory means that they typically don't have any kind of process-like abstraction and so run unsafe languages in a single privilege domain.

This project has now reached the stage where we have a working RTOS running existing C/C++ components in compartments. We will be open sourcing the software stack over the coming months and are working to verify a production-quality implementation of our proposed ISA extension based on the lowRISC project's lbex core, which we intend to contribute back upstream.



https://aka.ms/smallestcheri