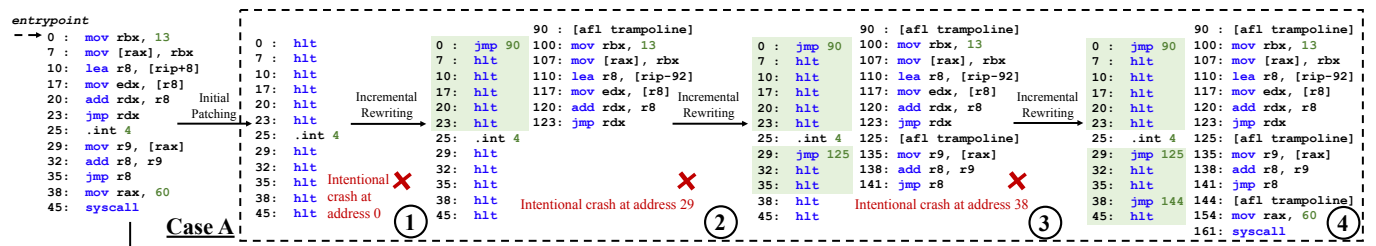
entrypoint
0 : mov rbx, 13
7 : mov [rax], rbx
10: lea r8, [rip+8]
17: mov edx, [r8]
20: add rdx, r8
23: jmp rdx
25: .int 4
29: mov r9, [rax]
32: add r8, r9
35: jmp r8
38: mov rax, 60
45: syscall
Initial Patching
Case A
0 : hlt
7 : hlt
10: hlt
17: hlt
20: hlt
23: hlt
25: .int 4
29: hlt
32: hlt
35: hlt
38: hlt
45: hlt
Incremental Rewriting
Intentional crash at address 0
1
0 : jmp 90
7 : hlt
10: hlt
17: hlt
20: hlt
23: hlt
25: .int 4
29: hlt
32: hlt
35: hlt
38: hlt
45: hlt
90 : [afl trampoline]
100: mov rbx, 13
107: mov [rax], rbx
110: lea r8, [rip-92]
117: mov edx, [r8]
120: add rdx, r8
123: jmp rdx
Incremental Rewriting
Intentional crash at address 29
2
0 : jmp 90
7 : hlt
10: hlt
17: hlt
20: hlt
23: hlt
25: .int 4
29: jmp 125
32: hlt
35: hlt
38: hlt
45: hlt
90 : [afl trampoline]
100: mov rbx, 13
107: mov [rax], rbx
110: lea r8, [rip-92]
117: mov edx, [r8]
120: add rdx, r8
123: jmp rdx
125: [afl trampoline]
135: mov r9, [rax]
138: add r8, r9
141: jmp r8
Incremental Rewriting
Intentional crash at address 38
3
0 : jmp 90
7 : hlt
10: hlt
17: hlt
20: hlt
23: hlt
25: .int 4
29: jmp 125
32: hlt
35: hlt
38: jmp 144
45: hlt
90 : [afl trampoline]
100: mov rbx, 13
107: mov [rax], rbx
110: lea r8, [rip-92]
117: mov edx, [r8]
120: add rdx, r8
123: jmp rdx
125: [afl trampoline]
135: mov r9, [rax]
138: add r8, r9
141: jmp r8
144: [afl trampoline]
154: mov rax, 60
161: syscall
4