Figuring out confusing assembly instructions — Koszek trick #2

W. Adam Koszek

Koszek ORG

wojciech@koszek.com

2022-10-05T17:47:04Z

Today's post will be very simple, maybe trivial. One of the hacks that I came up with, when I encountered confusing arcane of ANSI C, or when I played with assembly for fun and profit.

Problem: isolate ANSI C construct or in-line assembly block, so that upon a translation to intermediate assembly, block will be exposed more easily in a visual manner.

So imagine you want to isolate memory reference within ANSI C and figure out what the corresponding assembly line is. Assume given portion of the code:

"' [ptr.c]

#include <stdio.h>

int main(int argc, char **argv) { const char *str = "example"; char c;

(void)argc; (void)argv;

asm("/*