Research peek and poke

Minh-Triet Diep & Lars Jaeqx

In Datasheet-UM10326.pdf zoeken naar RTC zoeken (hoofdstuk 28). Register van RTC_UCOUNT -> 0x4002 4000.

Segfault als je dit wilt runnen in VM. Dit adres is op de host onbekend of niet toegestaan.

Op target runnen werkt maar in user space krijgen we niet de juiste waarde. Deze blijft statisch en geeft niet de realtime tijd. Omdat alleen via de kernelspace realtime access is toegestaan krijgen we wel de goede waarde als we het via de kernel uitlezen.

Verder dient het adres omgezet met io_p2v().

In de init maken we de "file" (/sys/kernel/es6/data) aan waar je vanuit de userspace in kan schrijven. In de kernel hebben sscanf(buffer, "%c %x %d", &command, &address, &value); gebruikt om de commando's uit te lezen uit de string die door de user wordt ingevoerd. Oom te lezen van dit adres zetten we het virtuele adres om naar het physical adres en printen we de inhoud. Het schrijven naar dit adres doen we door ook weer het virtuele adres om te zetten naar het physical adres en met memcpy de waarde schrijven. Als we de kernel verwijderen dan verwijdert hij ook weer de "file" (/sys/kernel/es6/data).

In de macro DEVICE_ATTR kunnen we de filename van de "file" aanpassen. Ook moet dan de " static struct attribute" de naam worden veranderd. We hebben hiervoor een define aangemaakt waar we deze in kunnen aanpassen.