如何在ARM Linux内核中使用硬件断点

03-27 22:57:22 凌空跃 阅读数 2763 ☆ 收藏 更多

ARM Linux内核中使用硬件断点

的CPU都支持硬件断点，也就是通过处理器提供专门断点寄存器保存一个地址，处理器在执行程序过程，会不断去匹配，可以设置成不同的模式来触发程序中断读这个地址或写这个地址， 并且可以设置长度，按8位，16位，或32位来触发。和软件断点比，好处是可以支持**读写断点**，程序断点不需要改写内存，可以设在执行前也可设置等等。

ARMv5架构以上都可以支持硬件断点，如是ARM9上可以支持2个，最新ARMv8规范指定2-8个。

Jtag调试器可以支持硬件断点，在Linux内核中，也可以支持硬件断点。

1.配置 CONFIG_HAVE_HW_BREAKPOIN

以3.18 Android内核上的ARM64为例，列举具体步骤：

在3.18上，这个配置没有写入menuconfig,所以首先修改Kconfig
kernel/arch/arm64/Kconfig.debug,加入

```
config HAVE_HW_BREAKPOINT
    bool "Hardware Breakpoint support"
    default y
    help
      If this option is hardware breakpoint
      If in doubt, say N.
```

2.在已编译过的Android根目录环境下：

```
make -C kernel O=../out/target/product/<chipset>/obj/KERNEL_OBJ ARCH=arm64 CROSS_COMPILE=aarch64-linux-android- KCFLAGS=-mno-android -j8
```

Kernel hacking”菜单下可以找到这一选项，同时还要把

```
Sample kernel code/Build kernel hardware breakpoint examples -- loadable module only
```

3.目前安卓内核都已经把模块签名打开， 为了方便调试，可能暂时关掉：

```
Main Menu/Enable loadable module support - Require modules to be validly signed
```

4.重编内核和bootimage,同进把samples module:data_breakpoint.ko也编出来

```
make -C kernel O=../out/target/product/<chipset>/obj/KERNEL_OBJ ARCH=arm64 CROSS_COMPILE=aarch64-linux-android- KCFLAGS=-mno-and
```

5.把的bootimage重新烧入手机，并且把data_breakpoint.ko也推送入

```
adb push /out/target/product/<chipset>/obj/KERNEL_OBJ/samples/hw_breakpoint/data_breakpoint.ko /data/test
```

6.这来就可以使用了，用法是插入data_breakpoint.ko模块，用符号作参数

```
insmod hw_breakpoint.ko ksym=totalram_pages
```

am_pages变量是内存总的页大小，在cat /proc/meminfo时会读它
会触发硬件断点，内核会打印中整个调用栈。

a_breakpoint.ko中，缺省是读写断点，可以在这个sample code的基础上，继续增强，通过不同的参数在使能只读断点或只写断点，包括长度。
于内核中samples/hw_breakpoint/data_breakpoint.c
W_BREAKPOINT_W和HW_BREAKPOINT_R来设置

```
static int __init hw_break_module_init(void)
{
        int ret;
        struct perf_event_attr attr;

        hw_breakpoint_init(&attr);
        attr.bp_addr = kallsyms_lookup_name(ksym_name);
        attr.bp_len = HW_BREAKPOINT_LEN_4;
        attr.bp_type = HW_BREAKPOINT_W | HW_BREAKPOINT_R;
```

文章最后发布于: 2016-