

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

声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
链接：https://blog.csdn.net/lingxf/article/details/50994645

ARM Linux内核中使用硬件断点

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，可以设在跳转前也可设置等等。

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。

gdb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。

配置 CONFIG_HAVE_HW_BREAKPOINT

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.
```

在已编译过的Android根目录环境下：

```
make -C kernel 0=../out/target/product/<chipset>/obj/KERNEL_OBJ ARCH=arm64 CROSS_COMPILE=aarch64-linux-android- KCFLAGS=-mno-android
```

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
```

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
```

重新编译内核和bootimage,同时把samples module:data_breakpoint.ko也编出来

```
make -C kernel 0=../out/target/product/<chipset>/obj/KERNEL_OBJ ARCH=arm64 CROSS_COMPILE=aarch64-linux-android- KCFLAGS=-mno-android
```

新的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
```

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

```
mod 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
就会触发硬件断点，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。
位于内核中samples/hw_breakpoint/data_breakpoint.c
IW_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-



所有人力资源公司排名

人力资源咨询公司排名

4939阅读

想对作者说点什么

如何给自己设置硬件断点（通过程序代码设置数据断点而不使用JTAG）

阅读数 7449

卓项目中碰到一个踩内存导致死机的问题，t

博文 来自：_xiao的专栏

Linux内核中设置断点

阅读数 511

on q1{set -x modprobe vfio modprobe vfio-pci echo 15b3 101a >/sys/...

博文 来自：mishuang2017的...

linux的gdb调试技巧

阅读数 637

主要演示了如何使用visual studio 2017开发Linux项目，并使用远程gdb调试NOTE：前提条件为vs所在PC机...

博文 来自：veson258的专栏

中设置读、写、执行的硬件断点

阅读数 1444

ichael Chourdakis, 翻译Binhua Liu 下载源代码 -56.1KB 简介 我是基于以下理由决定写一篇关于硬件断点的...

博文 来自：binhualiu1983的...



百度APP

全民战疫情 百度在行动

百度搜索疫情实时大数据

点击查看>



普华永道 人才招聘

普华永道 人才招聘

1707阅读

这些技术，你离BAT大厂不远了

阅读数 19万+

程序员都有一个梦想，梦想着能够进入阿里、腾讯、字节跳动、百度等一线互联网公司，由于身边的环境等原...

博文 来自：平头哥的技术博文

cSDN

原力计划

提升精英价值
释放潜能·助力成长

关闭