

他的回答

你碰到过的最难调试的 Bug 是什么样的？

wt.zzz



菜鸟一枚

YangminZ 等

补充一下，可能有人会误解，硬件组是在zedboard上开发的，zedboard有个arm硬核，使用0到256兆内存，除此之外zedboard还可以在加载一个核，也就是我们的cpu，使用的是256到512这一段内存

其次mips是指令集，是像x86这样的东西，似乎有人误以为是像linux这样的东西

最后，内核是我们编写的，而不是使用了某个Linux发行版，实际上前者比后者更容易。

---

这是一个在准备龙芯杯时遇到的bug，首先简单介绍一下龙芯杯（今年是第一届），龙芯杯需要每支参赛队伍在龙芯的开发板实现一个32bit CPU，使用的指令集是mips，决赛的时候除了CPU的性能还需要每个队伍在自己的CPU上展示一些东西。

我们学校一队展示的是超级玛丽和仙剑奇侠传，这两个一个是运行在FC上的一个是运行在DOS上的，跑在我们的mips指令集裸CPU上自然是不现实的，所以我们需要处理一下。

具体来说，先写一个简版的OS内核，然后写一个FC模拟器，这样也就可以跑超级玛丽了，然后再把SDLpal移植这个内核上，这样就有仙剑奇侠传了，当然上面都不是我干的。

我的任务很简单，调整OS内核，让模拟器能跑起来，比如FC模拟器获取设备信息（显示器大小之类的）需要读取/dev/dspinfo，刷新屏幕的时候需要写/dev/fb，获取按键、时间需要读/dev/events，这就需要OS去支持，以及一些系统调用。

本来我们的CPU是单任务的，没有mmu，但当时脑残的我非要加多进程，于是我就在软件层面加了个进程切换的东西，实现也很简单，在时间中断到来的时候，保存旧进程的内存镜像，把新进程的内存镜像拷到这个地址空间。

然后就出问题了，

因为要展示多个游戏，所以OS初始化完成默认加载/bin/init，然后这个程序会输出几个选项供选择，直到这里都还正常，但是进入游戏之后就会出各种各样的问题，当时观察到的现象包括 加点log游戏能正常运行，删掉就会挂掉，OK再加回来，mmp的又挂了，没关系再加log，又能运行了，然后稳定了一段时间，在什么都没动的基础上，又tm挂了。

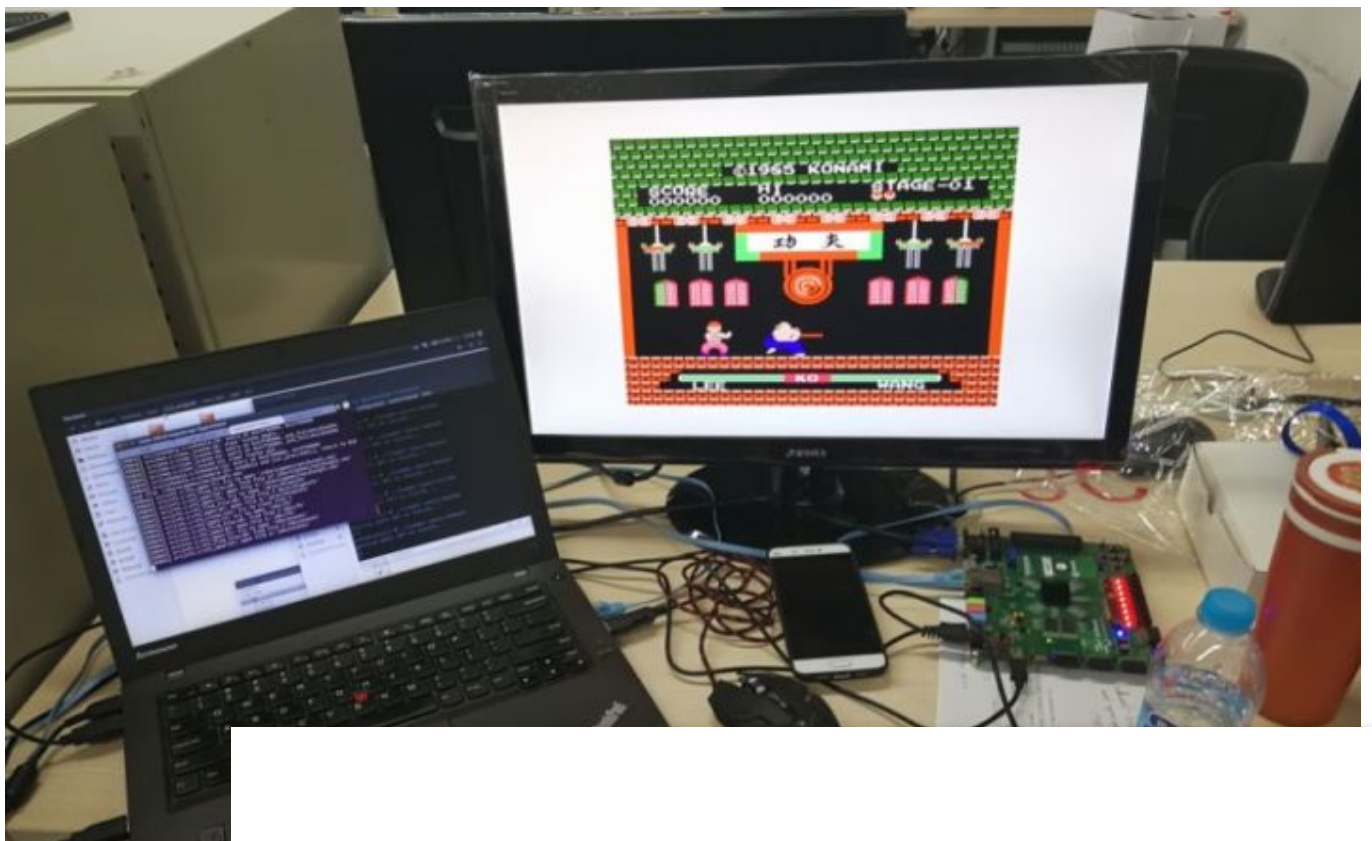
这个bug的蛋疼之处不仅在于加删log会改变运行行为，而且tm时间也会，而且错误位置不确定，出错现象不一样。通过加大量的log可以锁定出错的点在哪里，但那里只有一些初始化语句，而且有时候连log都没法输出完全。到这里为止我已经想过很多原因，包括输出串口卡死、某个地方内存溢出改了代码段、以及，，硬件组的CPU实现的有bug。说实话到这里为止我已经相当怀疑CPU有问题，但是凭空怀疑没有任何鸟用。

这个bug调到最后我整个人已经zz了，直到第二天晚上，我跟硬件组的人聊天才找出问题所在。

具体来说，硬件组为了性能考量，在cache的实现上做了一些假设，比如存指令的内存区域（对应真实CPU的代码段）是只读不写的，这条假设听着很合理，他们也就照做了，ICACHE不写回，对的，不写回，乍一听好像没什么问题，但是到我这里问题大了去了，前面提到CPU上没有mmu，所以我通过备份内存的方式实现了多进程，在实际操作的时候，这种方法需要频繁的修改用户程序地址空间的代码段。一开始加载/bin/init没什么问题，但后来腾给用户选择的的游戏的时候，需要将这个地址空间的指令换成游戏的指令，而由于ICACHE的实现，实际我往这里写的东西根本没有写到内存中去，不过因为ICACHE的大小限制，其实并不是完全没写进去，而是旧进程切回内核之前的epc指向那一小段内存没有写进去，其余地方还是正常的，所以当执行新进程跑到这段地址的时候，执行的其实是旧进程的指令！！由于时钟中断这种东西不确定，所以什么时候在旧进程的哪个地方切回来都是不确定的，这也就导致新进程运行到某个不确定的位置会执行一下旧进程的代码。。。

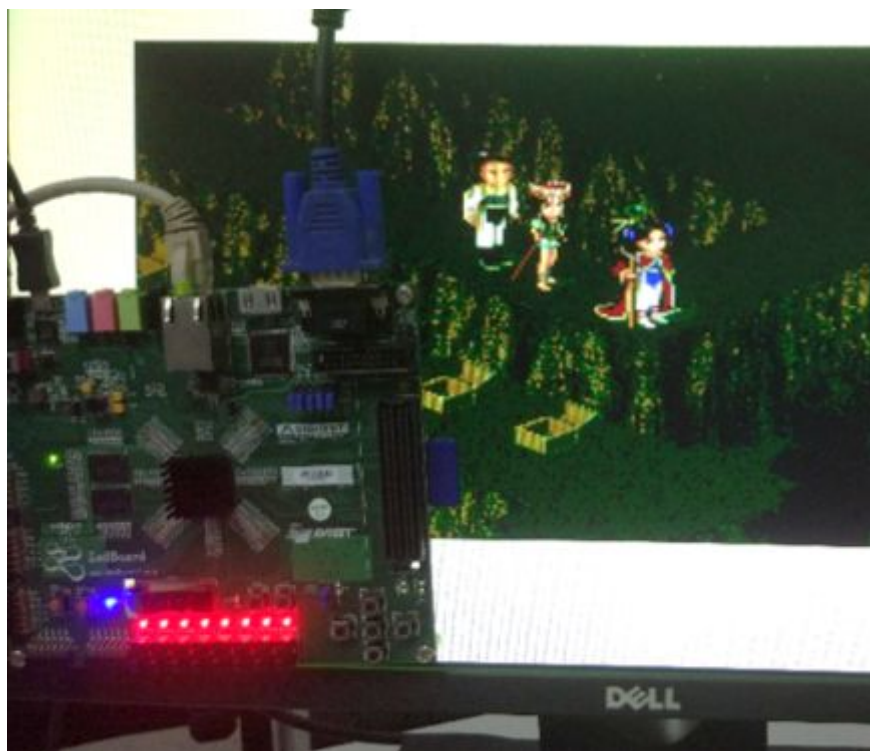
所以对于这样的CPU出了问题bug，究竟tm让我怎么调。。。

最后附上一张当时跑通的功夫小游戏：





以及仙剑：



编辑于 2017-11-12

#### 49 条评论



Month \

7 个月前

不明觉厉。。。



charon

7 个月前


突然想到PA。。



wt.zz (作者) 回复 charon

7 个月前


这个差不多是PA的后续，系统官方今年参加的比赛

 犹大的誓约  
游戏机?  
价格便宜么?


7 个月前

 wt.zz (作者) 回复 犹大的誓约  
把这当成游戏机的话，代价还是挺大的，一块开发版就得两三千，还得有人帮你写cpu、fc模拟器


7 个月前

 犹大的誓约 回复 wt.zz (作者)  
哦... ..那算了.


7 个月前

 Chen Moore  
这算是猪队友还是no zuo mo die...


7 个月前

 海边的卡夫卡  
膜拜大佬


7 个月前

 wt.zz (作者) 回复 Chen Moore  
其实主要是我自己作死-\_-b

7 个月前

 Warkeeper  
所以答主最后是放弃多进程，还是让硬件组的改实现( '▽` )

7 个月前

 wt.zz (作者) 回复 Warkeeper  
知道原因就比较

7 个月前

再见隐私协议

7 个月前



我也遇到过类似的问题，不过是在安卓上做hack时出现的。加了调试日志，一切正常，不加日志，一跑就挂.....

flylee

7 个月前



相比于我们脚本语言跑跑模型，写个高并发就感觉很高科技了，这才是真大佬

yy zz

7 个月前



试试通过给线程分配不同大小的栈，切换程序指针和栈指针来实现多线程

wt.zz (作者) 回复 yy zz

7 个月前



多线程还是很好实现的，因为的线程间共用代码，并且栈空间不重叠，没有mmu也可以搞定。主要问题是cpu上没有mmu，想要多进程就很蛋疼了。

无敌零桑受苦大魔王

7 个月前



装作听得懂的样子:]

王xx

7 个月前



这个板子是Zedboard吧，Zedboard上是ARM cortex和FPGA，ARM跑的是Linux，怎么会是MIPS呢？

icescream

7 个月前



这是龙芯的mips 开发板，怎么看着和zedboard这么像呢？话说xilinx也很喜欢拿那个超级马里奥demo.

wt.zz (作者)



zedboard除了

zedboard除了arm核，还可以在加载一下我们的mips cpu，不过这是我们开发用的，有arm硬核之后双率会提升很多，最后是要移植到龙芯的板子上的



wt.zz (作者) 回复 icescream

7 个月前

这不是龙芯的板子，开发是在zedboard上，最后迁移到龙芯的板子上

写下你的评论...