Segmentation fault 问题浅谈 2010-09-15 20:05:19

分类： C/C++

今天调试程序时遇到了一个问题，当我用 GDB 调试程序时出现了 Segmentation fault，以前没有遇到过，最后查看资料，有点明白了。

出现了 Segmentation fault，基本上的原因是，非法的内存访问。

例如数组的越界，在循环操作时循环变量的控制问题，也有字符串拷贝时长度溢出，指针指向了非法的空间，还有就是申明一个指针，但却没有对其初始化，就直接引用，或者没有开辟内存空间就释放内存，所以要检查申请空间时间偶成功。。。

还有那个问题在调试时会有这样的信息：Program terminated with signal SIGSEGV, Segmentation fault.

对于 SIGSEGV 这个信号，经常会和 SIGBUS 信号出现在一块，SIGBUS 与 SIGSEGV 信号的一般区别如下:

1) SIGBUS(Bus error)意味着指针所对应的地址是有效地址，但总线不能正常使用该指针。

通常是未对齐的数据访问所致。

2) SIGSEGV(Segment fault)意味着指针所对应的地址是无效地址，没有物理内存对应该地址。

通常导致段错误的几个直接原因：

1、解除引用一个包含非法值的指针。

2、解除引用一个空指针（常常由于从系统程序中返回空指针，并未经检查就使用）。

3、在未得到正确的权限时进行访问。

4、用完了堆栈或堆空间（虚拟内存虽然巨大，但绝非无限）。

这些是我个人的一些看法，希望和大家交流。。。