Android ELF文件got表符号偏移的确定

作者 Daemonceltics (/u/fa15f4e416ae) + 关注
2016.09.27 21:15 字数 335 阅读 40 评论 0 喜欢 1
(/u/fa15f4e416ae)

众所周知Android的动态链接器是linker，iOS是dyld，linux是ld-linux.so.2。由于同是linux内核，所以Android的linker与linux很相似，最大的区别就是linker不支持懒绑定，懒绑定的相关知识请参考我的另一篇博客linux plt 的实现(http://www.jianshu.com/p/ceb0381acade)。所以当Android的so或可执行文件在调用外部定义的函数之前linker已经把函数的偏移写到got表中，我们看一下如何通过ELF文件的结构获取到got表的偏移。

首先我要获取.dynsym .dynstr .rel.plt三个节的数据

.rel.plt和dynsym的定义如下：

```
typedef struct{
Elf32_Addr  r_offset;
Elf32_Word  r_info;
} Elf32_Rel;

typedef structelf32_sym{
     Elf32_Word    st_name;
     Elf32_Addr    st_value;
     Elf32_Word    st_size;
     unsignedcharst_info;
     unsignedcharst_other;
     Elf32_Half     st_shndx;
} Elf32_Sym;
```

获取.rel.plt每个重定位表所对应的符号的步骤：
1、使用ELF32_R_SYM宏（参数为.rel.plt的r_info）获取符号在.dynsym中的偏移
2、找到对应的dynsym在获取.dynsym的st_name字段，但这个字段不是字符串，也是一个偏移，是.dynstr节的偏移
3、通过偏移可以获取到相应的符号

以下代码来自于网络，是寻找got符号的程序实现：

```
for (i = 0; i < relplt_shdr->sh_size / sizeof(Elf32_Rel); i++){
    uint16_t ndx = ELF32_R_SYM(rel_ent->r_info);
    LOGD("ndx = %d, str = %s", ndx, dynstr + dynsymtab[ndx].st_name);
    if (strcmp(dynstr + dynsymtab[ndx].st_name, symbol_name) == 0) {
      LOGD("符号%s在got表的偏移地址为: 0x%x", symbol_name, rel_ent->r_offset);
      offset = rel_ent->r_offset;
      break;
    }
    if(read(fd, rel_ent, sizeof(Elf32_Rel)) != sizeof(Elf32_Rel)) {
    LOGD("获取符号%s的重定位信息失败", symbol_name); return -1; }
}
```

如果是一个静态绑定的符号获取方式就是获取.dynsym结构体st_value字段的值

```
for(i = 0; i < (dynsym_shdr->sh_size) / sizeof(Elf32_Sym); ++i) {
    if(strcmp(dynstr + dynsymtab[i].st_name, symbol_name) == 0) {
        LOGD("符号%s的地址位: 0x%x", symbol_name, dynsymtab[i].st_value);
        offset = dynsymtab[i].st_value;
        break;
    }
 }
```

以上代码出自Android GOT表HOOK技术 (http://ele7enxxh.com/Android-Shared-Library-Hook-With-GOT.html)

技术交流 (/nb/2910324)

Daemonceltics (/u/fa15f4e416ae)
写了 14550 字，被 3 人关注，获得了 5 个喜欢
(/u/fa15f4e416ae)

+关注

Android IOS 技术改变生活

如果觉得我的文章对您有用，请随意打赏。您的支持将鼓励我继续创作！

赞赏支持