山海狂心：仙古轩系列游戏逆向研究

@dontpanic

版本: 20230821 (b9790bb)
在线阅读：https://tuesday.dontpanic.blog

1 前言

妖弓计划是一个目标宏大的项目，我希望能够分别复刻《仙剑奇侠传》、《古剑奇谭》和《轩辕剑》系列游戏中的几款。当然，理想和现实还是有相当大距离的（笑）。

妖弓计划开始于 2019 年 11 月，从《仙剑奇侠传三》开始，当时还叫做 OpenPAL3 仙三开源版。我花了两个月的时间搭了一个简单的游戏引擎的架子，又在元旦和春节假期逆向了仙剑三的模型格式，成功完成了第一个 demo。我很享受这个过程，因为我对图形渲染和信息安全都有浓厚的兴趣，仙三开源版是两者完美的结合，它让我有一种我在 “快板界歌唱得最好，在歌唱界快板打得最棒” 感觉。2010 年 4 月 1 日仙三开源版发布了 0.1 版本，我写了一篇知乎文章，吸引了一些关注。

0.1 版本发布后不久，我突然得知可以通过某种方式获得《仙剑奇侠传三》的源代码。实话讲，这让我备受打击——之前所付出的所有努力似乎都变得一文不值，准备翻越的高山突然变得平坦。我本身不是一个凡事都追求意义的人，否则也不会开始做仙三开源版；但这件事确实让我低迷了很久，0.1 版本发布之后停更了一段时间。后来调整了一下心态，还是准备继续逆向下去，毕竟我还是在做没人做的事情，而且也是为将来做仙剑后续系列复刻做准备。

2022 年左右，[@0x7c13](https://github.com/0x7c13) 跟我过有一些沟通，他想用 Unity 做一版仙剑三。Unity 版的仙剑三进度很快，不久完成度就很高了，这就让仙三开源版继续下去的 “意义” 更少了一分，也让我显得有些执拗。所以我决定开启后续计划，启动其他游戏的复刻工作。只是觉得愧对《仙剑奇侠传三》主程序 [@Neil3D](https://github.com/Neil3D) 房燕良先生，仙三开源版 0.1 版本发布时也受到了他的关注和鼓励，现在我却要暂时放下仙剑三了。话说当时跟房先生联系的时候，我心里激动的不行，哈哈。

开始准备做仙剑四复刻的时候，突然想到《轩辕剑》有几款游戏也是用的 RenderWare 引擎，何不一起做了呢？ 又转念一想，干脆把《古剑奇谭》也加进来吧。目标还是可以定的远大一些，毕竟就算做不完也不会被人扣工资。既然目标变大了，之前起的名字 “OpenPAL” 也就不适用了。而且，保不齐以后还会有其他人也做仙古轩的开源复刻，我叫 “仙三开源版”、“仙四开源版” 就显得不那么精确，毕竟现在就有人分不清仙三开源版和 Unity 版。所以还是要起个名字。“妖弓计划” 就这样诞生了。

不论妖弓计划最终是成功还是失败，我都想让它留下点有用的东西，《山海狂心》就是其一，它囊括了我对各个游戏逆向分析的结论（目前主要是文件格式的分析）。互联网上也有前人的一些经验，例如 RenderWare 引擎就很知名，很多人对它进行了研究。但是由于诸如引擎版本不同等原因，很多时候分析结论无法拿来即用。还有一些软件可以解包游戏资源，但是并没有相关文档或代码描述如何解包。《山海狂心》试图总结我目前已知的内容，为所有对游戏复刻感兴趣的人提供便利。

dontpanic

2023 年 8 月，北京

2 打包格式 CPK

2.1 概述

CPK 是仙剑三、仙剑三外传和仙剑四使用的打包格式。CPK 打包格式支持保留完整的目录结构，支持文件压缩。仙剑三所使用的 CPK 打包文件没有任何的加密措施，而仙剑四则加入了简易的加密方式。CPK 文件整体格式如下：

内容	类型
CPK 文件头	CpkHeader
节点表	CpkTable
文件数据	...

其中 CPK 文件头中包含了 CPK 文件的元信息，诸如版本、文件节点数量、文件数量、节点表起始位置、文件数据其实位置等等。节点表中包含了所有节点的元信息，每个目录和文件都是节点表中的一项，它描述了文件数据的起始位置、文件的原始大小、压缩后大小、父节点、文件路径的 CRC32 值等等。值得一提的是文件路径的 CRC32 值是节点的唯一标识符，在节点表中也会使用父目录的路径 CRC32 值指定父节点。需要注意的是，CRC32 算法在 CRC 多项式表以及异或方式上有很多变种，在仙剑中的具体计算方式参见 crc.rs。

虽然 CPK 文件保留了目录结构，但是在游戏读取文件时，并不会真的生成层次化的目录结构，而是通过计算文件完整路径的 CRC32 值后查表得到对应的文件节点。例如，当游戏需要读取一个 CPK 文件包中的 `musiuc\P01.mp3` 文件时，首先会对字符串 “music¶01.mp3” 计算 CRC32 值，随后在节点表中查找该 CRC32 值对应的文件节点，从而得到文件的起始位置和大小。

CPK 文件可能会存在被加密的部分，可以通过文件头中的 `data_start` 字段的值是否为 `0x00100080` 来判断。如果存在加密部分，则自 CPK 文件头之后的 `0x1000` 个字节采用 xxtea 算法加密，解密密钥为字符串 “Vampire.C.J at Softstar Technology (ShangHai) Co., Ltd”。

妖弓源文件: https://github.com/dontpanic92/OpenPAL3/blob/master/yaobow/shared/src/fs/cpk/cpk_a

2.2 文件格式描述

2.2.1 CPK 文件头 CpkHeader

字段	类型
label	u32
version	u32
table_start	u32
data_start	u32
max_file_num	u32
file_num	u32
is_formatted	u32
size_of_header	u32

字段	类型
valid_table_num	u32
max_table_num	u32
fragment_num	u32
package_size	u32
reserved	[u32; 20]

2.2.2 节点表 CpkTable

字段	类型	说明
crc	u32	文件路径的 CRC32 值
flag	u32	
father_crc	u32	父节点路径的 CRC32 值
start_pos	u32	文件数据起始位置
packed_size	u32	压缩后大小
origin_size	u32	原始大小
extra_info_size	u32	用于存放额外数据，例如文件名