# 疯狂的程序员-第三十九章

原创

iteye_13777 于 2008-11-23 22:47:48 发布 74 收藏
分类专栏： 疯狂的程序员连载 文章标签： 金山 算法 虚拟机 Office 数据挖掘



自己做的东西，就是怎么看怎么满意，绝影和张厂长都觉得自己写的程序好，周总肯定要用自己的。

周总还是决定用张厂长的程序。绝影用汇编做的，公司以前没尝试过，他还是不想冒这个险，毕竟C语言才是入门语言，大部分程序都懂，以后万一出了什么问题要临时维护也不愁找不到人。

这个决定后来在很长一段时间里让绝影一直耿耿于怀。现在单位里特别是国有单位，年轻人往往对年长的领导腹绯很多，而上了年纪的领导又对这些年轻人意见很大，归根到底，人老了，不求有功，但求无过，凡事畏畏缩缩，又觉得年轻人办事不牢靠，太激进太冒险。

绝影原以为周总从国外回来，靠技术起家大刀阔斧创办这么个公司应该是年轻有为敢想敢做的人，当然公司创业初期周总也确实是这样，没想到公司过了最艰难的时候稍微稳定下来，周总的思想也开始陈旧。一方面要他负责技术减轻他和陈董的压力，一方面又不给他机会充分发挥他想法。

遥控器的CASE搞完了又要搞DAP，想起来绝影就头痛，暑假的时候燕儿在公司还要好点，现在开学了，燕儿也走了，周总就知道布置任务，验收代码，张厂长就知道摆弄他那堆电子元件，现在整个公司连个跟自己谈得拢的人都没有，苦水都没地方倒。

做这DAP就像打麻将，反正四川人爱打麻将是出了名的，说在飞机上听到麻将的生音就知道成都到了。

说到打麻将，在每把开始之前人人都是踌躇满志，想这把要和就和个大的，屁和？屁和根本就不和，至少也得和个大对子清一色的，还非得自摸，关三家，家家都关他个三翻五翻的。

这么想，等牌上手了，才发现原来生活并不是想像中那么美好。牌虽然是烂了点，好在自己技术还不错，总还是有点希望，于是按部就班地打，谁知是打啥来啥，越打牌越烂，烂到最后，算了，破罐子破摔，本来都已经到了绝望的地步，忽然发现自己居然和了个十三烂。

原以为DAP嘛，不过简单的C++封装，当初想得热血沸腾，真上手做了，才发现这样问题那样问题又冒了出来，既然问题都已经来了，没办法，想凭自己的技术尽量去解决吧，结果是修改一个BUG，又制造两三个BUG，越解决问题越多，弄到最后，这CASE估计就死了，没法做了。可是和打麻将又不同，打麻将打到最烂的时候还有个十三烂的和法，就比如日本流行的“败者复活战”，本来都败了，居然又可以复活，等于是天上掉下的机会。可是程序写烂了，又没有“复活”这么个机会。所以，写程序，前期不搞好设计，不写好文档真是害死人啊。

周总还是相当相信绝影，只说让他自己控制一下进度便进办公室去做他的事情，绝影自己在电脑面前倒是相当苦恼，这DAP确实是做不下去了，但是不做又不行，周总也没让他停下来的意思，而且他现在还肯定地认为：小绝啊，从来没让我们失望过。

于是绝影只好一边赖在电脑面前打发时间一边期待着周总又有新的任务交给他，没想到到真有这么一天，周总又对他说：“小绝啊，DAP是个长期项目，做到这里我们先放一放吧。”

周总这样说，他并不知道绝影心里的小九九，绝影却故意问：“怎么了？有什么问题吗？”

周总向他挥挥手，示意他进自己的办公室，在自己电脑上，他一面摆弄一个软件一边说：“也没什么。DAP这个平台性的东西，对我们来说是非常重要的，但是我想我们对应用上的开发也不要放了，毕竟这是我们近期收入的来源。我又琢磨着再做一些应用上的开发，最近我正调研一个软件——X-posure，用来计算骨密度的，这软件做得相当不错，可以外接扫描仪，直接把X光胶片扫描或导入进去就能将上面选定部分的骨密度计算出来。你看我给你示范一下。”

绝影对周总摆弄的东西并不感兴趣，他琢磨着周总这次要让自己做什么呢？莫非要模仿这个X-posure做个计算骨密度的软件出来？那难度也太大了。这也并非不可能，以前做KIPACS的时候周总就经常找些软件让他们模仿别人的界面。现在好多东西都

有什么包装专利、外观专利、防伪专利，你一专利了，别人就不能用，好在软件还没有这样那样的限制，所以周总就总找些现成的来让他们参考，自己又不是用户，又不是医生，要是让自己绞尽脑汁去想那界面该如何布置，那还不想死人。不过好像正因为没有这些约束，助长了不正之风，终于微软忍不住指责金山抄袭Office界面，那只是“抄袭”，谈不上什么“侵权”，不知道这事后来对周总有没有影响。

他点点头对周总说：“嗯，是很不错，那我们要做些什么呢？”

“最近我正调研这软件，举一反三，看看我们有没有什么可挖掘的，可做的，但这软件还是个共享版，老是要我输入序列号，否则就不让我接扫描仪，还有很多限制，不好调研啊。你上次不是帮陈董破解了一个PVT么？这次这个，你看能不能帮我破解了。”

绝影吃了一惊，严肃地说：“周总，这可是商业软件啊！”

“别着急别着急，我们又不搞商业用途，就是自己研究研究，法律上应该说得通的。”

绝影考虑了一会说：“嗯，那好吧，不过破解这个东西，我上次也说了，没有百分之百的把握，运气还是占了很大成分。”

“这个没问题，你尽量去做，做不出来大不了就不调研了。”

绝影从周总办公室出来，拷贝了一份X-posure，这才算个像模像样的商业软件，七七八八在安装目录中安装了一大堆文件。

上次那个PVT毕竟是绝影第一次做破解，虽然最后还是破了出来，但用的还是暴力破解，那是内行人所不齿的，弄得他自己都不好意思跟别人讲，暴力破解也确实不过瘾，找出一个位置把Jxx改成Jmp就行了。这次又来了破解的CASE，还是官方的CASE，当然要好好发挥一下。这么想，他打定主意，要么做不出来，要么就把注册机做出来，网上不是那么多牛人么？一会发布个XXX注册机一会发表篇XXXX破解笔记，你说自己牛，有什么证据？以前BOSS Liu在公司，天天跟自己明里暗里比技术，自己又确实比不过他啊，没有事实说话。这次要是把注册机做出来，也跑到看雪论坛去发一篇，东西放在那里，看你BOSS Liu这次还有什么话说。

这样美好的想像着，绝影开始破解起X-posure。

上次破PVT绝影给机器上装了SoftICE，结果弄得系统异常不稳定，新版本的DriverStudio在Windows2000下莫名其妙下不了断点，老版本的4.05还算好，可系统老是莫名其妙的重启，所以破完了就重装系统。这次却又得再安装一次。

破解本身不需要对这软件研究得有多透彻，只要知道他是哪个exe在负责输入序列号就行了，还是从MessageBox下手，思路不难，麻烦的就是这SoftICE。现在随便问一个搞破解的或者搞逆向工程的，谁不知道SoftICE？SoftICE牛不牛？当然牛。正因为太牛了，所以似乎专门给牛人用，或者只能给牛人用，因为操作实在太复杂了。IceDump这些插件绝影没装，就算装了他也不会用。你想从念大二第一次用SoftICE到现在，才学到勉强能用它调试东西的程度，你说要是再加个IceDump那还不知道得学到哪年哪月。

既然IceDump不会用，就用笨一点的办法，直接拿纸把前面的代码抄上，地址、机器码、汇编代码注释什么的都一字不落地抄下来再慢慢分析。

第一天做了些准备工作，第二天绝影开始认真的破解，本来作为一个程序员，在他身上是很难找到纸笔的，甚至久而久之很多汉字都只会用电脑打不会用笔写了。但是那一天，绝影却整整写了十六张A4打印纸的代码。张厂长在一旁有点不服气，说：“上次我打印个资料，才用六张纸，都领了个周总的口头警告，怎么你一会去拿一会去拿他都不说你啊？”

“我这是工作嘛。你以为我要是有废纸会去拿打印纸？废纸早让我做演算用完了。”

下班的时候张厂长叫绝影一起走，说是去泸州面馆吃面，绝影想了想说：“你自己去吃吧，现在正是关键位置，我要好好跟一下。”

“吃了饭拿回家再跟吧，现在肚子饿，一不小心就跟飞了，那损失就大了。”

“不行不行，家里电脑还是不要装SoftICE，不稳定。”

绝影说这些的时候头也没回，张厂长有点失望，不过想想也算了，他这种情况，多半是走火入魔了，现在不要说自己，就算燕儿肯定也喊不动他。

人都走完了，绝影干脆关了公司的门，十几张打印纸的代码铺在面前，眉目也有了点，毕竟那几年水平只有那样，再加上又是国外的软件，国外软件特别是成熟的大型商业软件在反逆向工程上一直都做得很菜这是公认了的。这跟国内形成了鲜明对比。在国内，随便一个“无敌剪贴板”之类的芝麻大点的软件都壳加了一层又一层，加了壳又压缩，压缩了又加壳，什么Anti-Debug，Anti-DAsm，虚拟机，花指令，密码学加密算法凡是能沾边的能用上的都用上，用不上的创造条件也要用上。比起他们，那X-posure的序列号算法确实算得上有失水准，字符有效性的判断都很简单，要么是0-9的数字，要么是“-”，关键的算法又全部写在一个函数中，找到这个函数基本上等于大功告成。

说起来也容易，但真的找到还是费了他不少心血。SoftICE用起来实在太复杂，现在搞破解的前辈教育晚辈一般都说：“SoftICE用过吗？我们那几年，只有SoftICE用，你那OllyDBG又如何？毕竟是三环调试器，你用着是方便，可是毕竟是三环啊，对付你的办法多得很，什么检测调试寄存器，什么Hook调试API，什么浮点指令漏洞，哪像我们那时候SoftICE基本横扫天下。所以啊，工具多了，人就懒了，要学真技术，还是要在Kernel上多下点工夫啊。”

所有位置找到，绝影开始琢磨这个注册机，想明天到了公司，周总问：“小绝啊，工作进展如何啊？序列号找到了吗？”他就大大咧咧拿出这个注册机说：“还行吧，注册机也写出来了，你用用看行不行吧。”这样，周总肯定又要对他刮目相看，肯定又要拍拍他的肩说：“小绝啊，从来没让我们失望过！”

其它什么难的，就是那个关键函数，虽然汇编代码不是很复杂，但这明显是高级语言写的，那些数据的计算要还原成C语言代码还是麻烦，想起网上一篇文章，好像就是介绍直接用Windows优化大师的反汇编代码写注册机，给了点思路，不如就直接用汇编语言来写注册机得了。

这样一直忙到晚上三点多，绝影用自己写的注册机生成了三个序列号，居然都能用。他才收拾好打印纸出了公司。

街上的店差不多都打烊了，只剩几家烧烤店，绝影去了离自己住处最近的一家，喝了两杯豆奶，吃了两条烤鱼，想起以前跟BOSS Liu在这里喝酒吃烧烤，自己这个CASE算是做完了，几百块的奖金基本上算到手，不知道他在成都混得如何。

回到家，绝影还是没有一点倦意，他也不想睡，现在睡了明天肯定又起不来，于是拿出写满代码的打印纸，整理好思路，打开Word，题目写上《X-posure序列号破解》，写完这篇又花了两个多小时，于是在看雪论坛上注册一个ID发上去。

看雪论坛在搞破解的人当中那可是技术的圣殿啊，所以他还算比较人道，可以不注册就去看帖子，绝影也一直没有自己的ID，这次要发文章了，才去注册一个。没想到几天以后，这篇帖子居然被看雪大大批准为精华贴，更没想到，几个月以后，这篇帖子竟然收入了《看雪论坛精华》。

绝影洋洋得意看着自己论坛上面帖子：1，精华：1，想以后要么不发，要么就有成果了再发，发就发精华贴，100%看雪论坛精华，还说我不牛么？

这么想了，所以从那以后，绝影在看雪论坛上始终只有一篇帖子。