Neurohazard

【flashsky@瀚海源/阿里巴巴集团安全】我的安全之路

發表於 2018-01-01 | 分類於 信息安全 |

关于作者简介

FlashSky，闪空，真名方兴，黑客界最励志的传奇人物，市场营销学出身，当过银行柜员、开过酒店，29岁才进入安全行业。漏洞挖掘能力一流，尤擅诗词格律，人称“诗洞双绝“，著有文章《我的安全之路》，非常励志，希望有志于从事安全行业的年轻人将它读十遍。曾有机会肉身翻墙去美国，后放弃。闪空是国内APT行业的开创者，也是最早APT的受害者。当时他为美国EEYE工作，与美国同行玩hack game，比拼谁发现的漏洞多、危害度高，据称闪空的漏洞挖掘能力碾压美国同行，引致对方不爽，对方利用漏洞远程持续攻击闪空家里的路由器，使得路由器发热并最终引发火灾，闪空差点当了邱少云。这是真实存在的案例，网络世界，只有你想不到，没有做不到。

简介摘自 中国黑客群侠传 安全龙 安全龙

Flashsky:我的安全之路
https://im1gd.me/2017/01/30/Flashsky-%E6%88%91%E7%9A%84%E5%AE%89%E5%85%A8%E4%B9%8B%E8%B7%AF/

引子

很早之前，KILLER曾经劝我写写我的安全经历，因为我是从计算机零基础开始自学计算机和安全的，这些经历可以帮助很多后进想学安全的人少走很多弯路。当时太忙，而且做技术工作时，觉得自己写自己未免有自我吹嘘的嫌疑，所以也就没有动笔。

10年开始和王伟一起做翰海源，角色逐步由技术研究人员转化为管理人员，最大最有挑战的工作就是打造技术团队，以及如何向这些后进的人员传递自己的知识和经验。深刻感觉到自己以前的这些经历，或许可以帮助这些同事和希望从事研究安全的人员。所以就有了此文，主要目的有三:

1)是给那些希望从事安全比较低层研究的人以激励,其实用心去做一件事,取得成绩并不难.

2)是很多事情会随时间而淡忘,有些事情会被一些报导所混淆,现在记录下来,未来也有个参照

3)是有很多人对我有很大帮助的,是应该我感谢的,在此文中表达对他们的感谢

希望能对各位有所帮助。(以下都是我个人真实的经历,但是考虑到会牵涉其他人和事,所以一些地名公司名人名都会做些处理)

0x00 大学时代：计算机补考请人代考

我高考时数理化生都是高分，但是语文政治英语都不及格，勉强过了少数民族地区的照顾线，进了湖北XX学院。本来报的专业是物理，但是被调剂到市场营销专业。

上大学之后，没有了父母的管制，对学的课程也没什么兴趣，加上那时候都是包分配，没什么压力,于是开始完全放纵自己，每周去课堂的次数屈指可数，我一天的经典日程安排是：早上起来，和对门的一个业余四段下围棋（我当时的棋力大致是业余三段左右，他也是逃课大王），一般下到中午两三点左右才结束（我和他都是长考派，中午吃饭由观棋者带饭），然后出门踢足球。晚饭后，以打台球和打电子游戏为主。

这样下来，毕业那年，成绩自然非常惨淡，靠抄袭和作弊，最犯难的几门如英语什么给混了过去。但是还是遗留下高数，统计，计算机三门需要补考。我寝室的的另一位姓杨的逃课大王（他爸是当时有名的律师，靠在S市专门给人打经济官司发了财，在S市开了一家公司等杨同学回去经营，所以他在学校天天的事也就是玩和等毕业,他个子高,喜欢打篮球）也只需要补考两门，统计和高数。于是我和他统一行动，先是找到教统计的老师，统计老师是一位女老师，这位杨同学于是向其哭诉，我们都是来自大山区的穷孩子，借了很多钱才读大学的，现在要是补考不过毕不了业，家中老母都要自杀之类的话，说的声泪俱下，说到那位女老师都跟着只掉眼泪;我才知道这位仁兄不去从事演员行业真是浪费人才，于是我们顺利的搞定了一门。

高数，则遇到了些麻烦，负责高数的老师是有名的铁面无私。于是我们补考也没过，只剩下最后离校前的一次机会了，我和他在教室里一间间寻找教高数的老师，希望能问到教我们高数老师的家，然后上门去求情，正好看到阶梯教室里一位教高数的老先生刚下课，于是杨同学跑上去询问，这位老先生沉着脸问：你找X老师干什么。杨同学也直白，直接说为补考的事，这位老师脸色大变，厉声问到：你们怎么知道我是这次补考的出题老师？我和杨同学心理一惊，真是得来全不费功夫啊，居然这样都给我们误撞到出题改卷老师了。于是求情了半天，但这位老师好象一点都没受到感动，一副铁面无私公事公办的样子。于是我和杨同学只能铩羽而归。杨同学不死心，出门居然找人打听到此老师的住址，于是撺掇我买点礼物上门去求情。于是我和他买了几斤苹果和香蕉，由于只打听到该老师住址的楼栋和单元，并不清楚楼层，所以他负责打前哨敲门去问。我在后面远远的拿着水果跟着，两人鬼鬼祟祟来到该老师住所。他敲了一楼的房间问是不是该老师的住所，出来一老太说该老师住在2楼，于是我们上了2楼，敲门一问果然是此老师的住所，老师正好不在，只有老师老婆在家，我知道这事八九成了。因为这位杨同学对付三四十岁妇女的杀伤力指数绝对一流，又高又帅又会说又能演，道明来意后，杨同学开始了入戏的表演，果然不久,这位师母就开始掉眼泪了，最后师母说：你们太不容易了，这事包我身上，把你们名字记下来，老头子回来我给他说，他要难为你们，我就让他好看！我们千恩万谢退出来之后，相视一笑。看来天无绝人之路啊。

剩下计算机，只能靠我自己一个人搞定了，计算机不是我们的主要课，当时主要是学的DOS操作和BASIC语言，所以考的很简单。但对我这种一次课都没去上，只是去上机打了几次游戏只会DIR和CD两个命令的我，自然是难如登天；不过计算机不是主要课，监考不会太严。我的上铺是我的老乡，家里比较穷但学习好，我从入校就经常接济他，这个时候他自然就主动请缨要帮我代考。

于是这样，我三门补考都被对付过去，94年的6月，我光荣的毕业了。

0x01 X王工作之酒店经理一(94-95)

我毕业去的企业,是湖北很早就上市的一家以焊条起家的公司X王，他是一家民营企业，由于焊条做的不错，然后就成了X市里的一面红旗，于是很多破产或经营不善的企业都由市政府出面盘给X王兼并，X王再以这些兼并企业的资产去申请贷款然后到处布点，至于这些兼并的企业是否真能因为X王的兼并扭亏为赢做起来，就只有天知道了，但是X王却成了市政府不敢让其倒下的旗帜，因为一倒，全市一半的工人要失业。我去的那年正是X王宣传要三百大发展的时候，所谓三百就是三年内要在全国建100家焊条厂，100个销售公司，100个其他实体，于是那年招了近万名的毕业学生，具体分配到不同公司的大会上,只要你敢说去做，就马上给你任命和一笔启动启动经费，让你去各地开始建办事处等机构然后去申请当地贷款之类的。我不太能忽悠,所以最后我去的企业是X王兼并的一家本地的柴油机厂下面的三级房地产公司，那个时候，房地产还没有起步，远没有现在这么

热火,所以轮到最后选人,就这样我去了这家公司。公司老板姓姜，通过关系把柴油机厂里面的地拿了一块，就在柴油机厂里开始盖商品楼，我刚去的时候，在工地上泡了几天，然后就被抽回来做文员，当时还是按学历和工作年限拿固定工资，我记得我是120块左右，不够我吃盒饭的（当时此地因为修建某千亿的大工程,导致本地物价带的很高，比省会武汉还高，盒饭素的2块，荤的3块）。每个月还得找父母寄些钱来才够用，不过公司管理也很混乱，也没什么人管，上班经常几个总都带头打跑得快，下班后打球打麻将就成了经常性活动。我这个新手，自然经常工资刚到手当天就输得只剩下一半，然后只能编理由去找父母寄钱，然后省着吃馒头过日子，不过老板是个喜欢到处喝酒的人，我当时刚从学校出来，经常打球，身体不错，酒量白的有一斤半以上。于是老板就经常带我们几个能喝的出去找领导朋友什么的打酒仗搞关系，就这样凑合着也能经常打打牙祭。当时也很惶惑，觉得这样混日子实在不是个方法，宿舍里住了我的一个同班同学，他是个计算机迷，拿过学校计算机编程比赛的第一名，天天捧着一本计算机书看，劝我自学计算机，于是我借了他一本计算机的书，看了2页就头疼无比，把书还给了他，对他说我实在不是学计算机的料，这辈子估计都不会和计算机打交道了。N年之后，他也出来在武汉的一个计算机公司做应用开发，我去武汉见同学时碰到他,当他知道我现在从事计算机安全研究时无比惊讶，我相信应该是当年我那种决绝的样子给他的影象太深了。

3个月之后，原来的老板被斗争走了,传闻那楼当中的一栋老板卖给一家公司了,但对方开价是出600万,但最后居然400多万成交的,于是公司有人向上面举报,姜老板就被调离了，新上台的老板是一直被我们认为是工人出身的老好人老刘,给我们的影响就是躲事,从不得罪人,对什么人都笑呵呵,除了打牌时赢了之后说话比较大声外,平常说话都怕惊了别人的刘副总，上台之后，才发现原来老实的刘副总并想象那样温吞，后来想想,或许举报姜老板背后也可能有他的影子.公司又成立了一个子公司叫XX物资公司，说穿了就是倒卖物资,特别是钢材，我也调到这个公司来。其实没什么事，就是四处打听倒卖信息然后倒卖，一帮人除了天天打牌赌博之外，就没做成几笔生意，不过隔壁的一家做钢材老板的儿子，倒是让我第一次见识了吸毒的危害，这个老板辛苦了多年有几百万身家（94，95年的几百万可不是小数），可惜把儿子惯的吃喝嫖毒无所不具。天天都带一个姑娘回来睡，经常逼父母给钱做毒资。有一次钢材老板发飙决定不给，他儿子居然拿刀架钢材老板的脖子上说：我这辈子，姑娘玩了数百个，现在死了也不亏，你既然生了我，财产迟早都是我的，你心疼个什么，早点给我我们相安无事，惹急老子了把你杀了也没什么怕的。钢材老板最后只能服软，毒品真的能让人变成魔鬼。

这家房地产公司原来还投资了一家太白酒楼，一位姓孙的同事去主持做酒楼经理,该同事是我见过最精的人之一，估计折腾了些钱，于是抽身而退。于是在物资公司呆了2个月后，房地产公司让我去接替这个酒店经理的职务，理由是我是学市场营销的，给我机会大展宏图，于是我真以为是领导看重，屁颠屁颠的就走马上任了。上任后，才知道为啥让我这个新人来了,因为前任留下了巨多财务窟窿，很多货款没付，不付请欠款,人家都不卖货了,天天都有上门讨债的人，当时我才毕业也没什么心眼，于是找父母要了几千块，自己补贴了进去，终于让酒楼可以运转起来了，那知又给电力局停电了，到电力局一问，才知道前任从上任起就没缴过电费，电费带罚款什么的居然累计到两万元了，这个数目，我也没法再向父母伸手要了。不过，电力局的总工经常到我们这里吃饭，和我们这里的一位服务员聊的不错，于是这位服务员给我出主意，请电力局的总工和手下吃饭，再每人送条烟，看能不能减免。没办法，只能低声下气来到电力局，向这位总工表达了请吃饭的意思，还好，这位总工很爽快答应了。下班后电力局的来了20多号人，整整两桌，总工意味深长的对我说：小方啊，我们喜欢梗直的人，你看着办吧。我知道这个时候，是我上场的时候了，上去客套了一下，换上5钱的白酒杯，2桌，3圈，中间不歇一口气，打下来之后我也快醉成烂泥了，但强撑着直到饭局完毕,那位服务员给电力局的每个人把烟递上，他们收下。总工最后走的时候，拍了我一下说：小方，够意思，你明天来电力局申请一个新电表，我们给你出个证明，就说以前的坏了，导致电表计数错误。这样你只需要付几百块就行了，送他出门后，我一下就瘫在沙发上睡着了.

0x02 X王工作之酒店经理二(95)

酒店终于能正常运转了，我这个刚从学校出来的职场新人开始见识到更多的社会现实。首先是对门的老板跑过来,找我商量双方的服务员互相为对方提供“特殊服务”，意思就是双方都准备或招聘一些小姐做服务员，当对方客户有需求的时候就可以互相帮助联系，可以避免尴尬和被人举报，我自然装糊涂没搭理，其次就是我的新老板刘总，经常过来从酒店提些物资走，自然不打条子不给钱，不过这个我觉得也能忍受，或许老刘还怪我没主动去给他送呢。另外就是经历了第一次朋友的背叛，我没当酒店经理之前，旁边住着一个转业的军人在厂里当工人，是我老乡，家境不好，还带着一个没工作的妹妹，所以我经常把我不多的工资资助一半给他，自己去吃一个月的馒头。当了经理之后，刚开始每天货物的采买都是我经手，但后来事情多了，也想给他找个多增加收入的方法，采买一般都是大清早,也不耽误他正常的工作,于是就聘他给我做采买;一天晚上我陪客人喝酒喝多了出来吹风，偶然看见他和一个人在墙角嘀咕，听见有什么价钱之类的话，我于是走到隐蔽处听，原来另一个人是个菜贩子，他们正在商量如何做价格好欺骗我赚中间的钱,这位转业军人,我一直认为他很正派,也一直把他当大哥看,居然也是这样,我当时心痛得无以复加.我默默的回房间,过了几天,我以酒店亏损为理由,说老板要我精简经费,采卖都由我自己操办为由,把采购收了回来,他好象也发觉了什么,或者是对我怀恨在心,从此后再也没有来找过我了.

在酒店,拼酒几乎成了我最主要的工作内容,此地风俗喜欢喝斗酒,于是老客人来,上面公司的业务宴请,我都得出面来应酬.经常都是四五两左右的大玻璃杯,倒满白酒整杯地抽下去.我状态最牛的一次,就是元旦哪天喝了三顿,中午晚上两顿都超过1斤半,中午和客户喝,下午上级公司聚餐,到了晚上10点,我们酒店自己聚餐,2个厨师看我喝了不少,就想放倒我,于是倒了一满玻璃杯白酒,碰了我杯子一下,然后一口抽了,按本地风俗,碰了杯子的酒对方抽了你也必须一口抽,我没办法,只能一口也喝了下去,但最后居然我没倒,这2个厨师却倒了.

很快春节就来了,酒店需要有人看店,于是我放了所有人的假,自己留下来看店,这是我第一个没和家人一起过的春节,真寂寞啊.公司一位姓邓的同事,除夕晚上跑来看我,小邓是东北人,也是超级能喝的主,带来了5瓶白酒说陪我过除夕.我打开冰箱一看,只剩半只鸡了.于是瞎烧了一个火锅,2人就这样把5瓶白酒给喝了下去.我喝完后一边说话,突然间就睡着了,小邓居然还能把我扶到沙发上,自己回家了.第2天醒来,对门酒店那个要和我交换服务员特殊服务的老板远远看见我连忙跑来,对我说:小方小方,你赶快去医院.我说咋了?他说你太阳穴附近通红通红的,是不是脑溢血了.这是我第一次伤酒,接着春节时一个家在附近农村里的服务员请我去他们家喝酒,那边农村喝酒就是拿所有客人送的酒出来一起喝,于是你每一杯倒的酒都是不同的牌子,杂着喝,我拿了一个2两的杯子,3杯之后换了不同的三样白酒,加之前几天才大醉过,于是现场直播,2次伤酒之后,我的酒量于是急速下跌,到现在我喝2两白酒就不行了.某次回老家,被表妹和表姐夫灌了一杯2两的白酒,回家之后就吐了一个晚上,而他们当年都是在不知我深浅的情况下,想灌我结果被我灌倒在亲戚中成为笑谈的主,风水轮流转啊.不过酒这玩意就是靠身体,这是我多年的经验,还是要多多爱惜自己身体,不要象我当年这样.

春节过后,酒店又回归了正常业务.夏天的时候,一天刘总陪着他的上级公司的办公室主任来吃饭,这位办公室主任一副道貌岸然的样子,我刚工作的时候,在走道上和一位同事说话大声了一点,他走出来义正言辞把我们好好训斥了一翻,但现在酒桌上,则完全是一副江湖上兄弟的套路,一直暗示给我说:以后要在酒店多给他们一些照顾,肯定会对我很好的.当时我没太明白照顾是什么意思,以为也就是如老刘一样,让他多拿多占一点物资或者白吃几顿,所以就含混着答应了.不过后面马上就知道照顾的含义了,当时的酒店,卡拉OK正在流行,我们的包间都是带卡拉OK的,经常有些老客人吃完了饭,撤下桌子要服务员陪唱歌跳舞之类的,一般这些老客户和服务员都比较熟,虽然经常口头上占些便宜,但是手上还比较老实,不会太过分,所以我也会满足这些客户的要求.自然刘总和这位办公室主任吃完饭后,也要求服务员陪同跳舞,但是不久之后,几个服务员就哭着下来对我说,这些人对她们动手动脚.我于是让服务员都回家了,酒店只剩下我和几个男厨师,刘总和这位办公室主任在上面拍着桌子发着酒疯叫服务员,我于是走上去说:已经过12点了,明天酒楼还要营业,我让她们都回去先休息了,你们有什么需要叫我,我给你们服务.这2人于

是吼着说:那你负责给我们找一些做特殊服务的人来.我当时血气方刚,针锋相对说:你们领导让我到这里是来做酒店的,不是拉皮条的.你们自己叫吧.刘总和这位办公室主任于是把桌子一锹,扬长而去

0x03 X王工作之下岗(96)

再不经世事的人,也知道我这个酒店经理,肯定是做到头了.

不出所料,过了2个月,我首先是从酒楼以工作需要之名调回了物资公司.又过了几个月,公司优化人力资源,我成了被优化对象;被优化的对象都送到X王总部,重新安排工作,我被送到X王刚兼并的一个大山里的农用厂先当工人.按计划是让我折腾一个月后,熟悉了一些常见的业务和名词后,我将成为销售人员去售卖农用车给农民.

这个农用车厂,几乎已经停产了,但还有一大批农用车库存,但都是有问题的车,很多车都开不起来.但是前面出去的销售人员居然也能靠连哄带骗把他们卖给一些外地的农民,然后从这里提货,于是我们干的最多的活就是把这些开不动的车先从库房推出来,然后搭块扳子,靠人工推上发货的卡车上,然后发给那些上当的农民. 我在想,这些用了一辈子积蓄买到开不动的农用车的农民,拿到车之后会是怎样呢?但我没时间去想他们更多,因为这是我生命中最黑暗的一段日子,优化之后工资停发,我身上就10多块钱,厂里食堂也停了,天天去老乡那里套点老乡的红薯吃.心肠好的老乡,不要我的钱,比较计较的老乡,就给个一块或者五毛.晚上山里下着鹅毛大雪,住的地方没有被子和床,只能找些稻草回来铺在地上,实在冷得受不了,就去外面拾些柴火回来来烧,虽然烟子熏得眼睛实在受不了,但好歹能对付过去.但隔壁一个人,因为烧柴火把稻草烧起来引发了火灾,虽然被及时扑灭也没引起伤亡.但是这点取暖措施也就被禁止了.在这里过了1个多星期,我每天冻得睡不着的时候,都在想,未来我会是怎样呢?就是这样活着吗?我能改变什么吗?但我很快就沮丧的发现,未来我可能会更惨,很显然,给我的小鞋不会因为我的努力就停止,这样的生活我必须改变,但我怎么改变呢?继续呆着当着没有出头之日的推车工或者去当欺骗农民买开不动的农用车的销售人员吗?我想我良心无法接受,回家吗?考大学本来我父母就不同意,因为我的母亲姐姐姐夫都是银行系统的,当时银行是可以照顾家属进银行的,所以他们要我去读银行的中专然后进银行,但我讨厌银行刻板的生活,还是报考了大学,希望能混个人模鬼样,而我父母几个同事的子女,学习差的一塌糊涂,高考只有一百多分(总分710),最差的学校都上不了,但是靠关系上了银行的中专,出来分配到银行工作,一个个混了段日子都升成小管事的了,那个牛逼啊.我就这样灰溜溜地回家,亲戚朋友会怎样看我呢?而且我回家之后,放弃了已有的工作,什么都不懂的我又能做些什么工作呢?

我在稻草上,几个晚上都没睡着翻来覆去地想,对未来生存的恐惧让我深深感觉到,一个人要没有生存的技能,在这个世界上是多么无助.我开始后悔在学校里荒废掉的时光.

帮我最后下定决心的,是旁人说起的一个新闻,那几年,正是工人大下岗的时候.X王兼并的一家厂子,最后还是支持不下去了,于是这个厂子的工人就全员下岗了,停发工资了.一对中年夫妻都在这家工厂做工人,于是家庭一下断绝了经济来源,他们还有一双在读书的儿女.他们想去找工作,但是身无所长,找不到工作.于是绝望中,杀了自己一双儿女后双双自杀.我被深深震撼了,难道,我的未来也要如他们一样?当一个身无所长的工人,到中年的时候,突然接到下岗的通知,找不到工作,然后等待悲惨的结局?不,我还年轻,我应该还能改变什么,而不是等一切都来不及的时候,被命运和世界主宰.

第二天,我一早就爬了起来,从工厂坐了个回X市的便车,找同学借了些钱,然后什么招呼也没打,连我在X市宿舍里的被子,行李,我大学心爱的用我2个月省下来饭钱买的一把黑吉他都没带.买了回家的长途车票,头也不回的离开了X市.自己给自己主动下岗;回到了家乡.在我的父母充满惊讶的眼神中,告诉他们,我决定不在厂里干了,我要自己找工作打工.

多年以后,我对X市的记忆日渐模糊,除了因为回家偶然途经之外,再也没有去过.只有一次去武汉中途到此地转车,离转车开车时间还有4个多小时,我抽空又来到这个房地产公司的旧址,当年我们盖的楼已经入住满了住户,也开始

显得有些老旧了,转过楼道,我依稀还看见那位办公室主任走进单元.可是除此外,我没看到一个其他认识的人,于是我又默默的离开了.今天,我回想起当年这些,依然还能感觉到当初自己,被对生存和未来深深的恐惧占据心灵的感觉,我想我或许应该感谢刘总和那位办公室主任,是他们的小鞋让我终于惊醒,让我在还能靠自己努力去改变命运的年纪,选择了一条不同的道路.不然,或许某天,社会新闻里出现的一位下岗失业自杀的新闻人物就可能是我.

0x04 四处打工之信用社出纳(96)

父母是最心疼儿女的,在这个时候,他们四处活动,希望能帮我找到一份工作.靠母亲老银行的关系,不久后找到一个去农村信用社当聘用制出纳的工作.在这之前,我表达了我想学计算机的想法.我姐夫是工行电脑科的,也是科班计算机专业毕业的,就在银行里找了一台报废但还能用的386的机器给我,抱这这台黑白显示屏的老机器,我开始了自学计算机之路.我姐夫把他大学里的计算机教材找出来,就成了我自学的教材.我用飞速的速度首先学会了打字和DOS基础命令操作,当年正好是各个业务系统都开始上微机的时候,会打字出去找工作是一个很大的优势.去信用社当出纳,还必须考点钞手法和算盘,在压力的驱动下我居然几天就精通了它们,于是通过点钞和珠算考试之后,我成了农村信用社的一名出纳.

这个时候,我开始了我自学计算机。这是最艰难的时候,我姐夫是学硬件的,先开始我想跟着他学计算机维修,但很快我发现,我还是对软件和开发更有兴趣点,当初银行系统都是类UNIX的xenix系统,于是开始学xenix的操作与命令.这些都容易,最难的还是学计算机组成和操作系统原理,由于我姐夫是学硬件的,他的计算机组成和操作系统原理的教材,都是以汇编做例子来讲解的,对于我这样一个没有任何语言基础的人,想看懂这些汇编级的计组和操作系统原理的教材,其难度可想而知.我咬着牙,一遍又一遍的看,看不懂的,先记下略过.下次再看,每条指令,先从英文的角度去理解他的意思,就这么着,一遍一遍,我不记得这两本书我看过多少遍,但最终,我都看懂了.想来这或许是一个奇迹，但我宁可相信是对未来生存的恐惧驱使我获得了某种力量；未来我从事安全研究的汇编功底,或许就是这么来的吧.看懂了计组和操作系统原理这2本书,我发现我对计算机系统和语言的理解能力大副上升,我于是买来计算机高级程序员考试的教材,自学数据结构,FORTRAN和C语言,有了计组和操作系统原理的汇编根基,C语言中的指针这些很让人饶头的概念就很容易被理解了.

信用社的工作对我而言很轻松,但是对信用社其他的人就不一样了,她们基本上都是银行系统的女家属,年纪都比较大,新上的微机系统的操作和打字显然对他们是个很大的挑战,每笔业务都需要做很长的时间,而我则非常的快,自然我成了她们的威胁,每当我干完出纳的活抽空去看计算机的书时,而她们还在不知道怎么敲打字的时候,她们就会很自然的嘲笑我一个出纳还看这么高深的书,难道想一个人把活都干了之类的话,我也就当耳边风.不过另一个人让我更讨厌,就是社长的司机兼系统管理员.信用社没有搞计算机的专职人员,信用社这套柜员操作系统是武汉一家公司来安装调试的,是当年流行的NETWARE的系统,我们那里山高水远,那几年路也不好走,每年都会发生大客车翻车重大伤亡事件,所以那些武汉的人当然不会经常到这边来维护,于是就把一些日常如开机关机命令写好,让这个司机每天定期照着做,于是这个司机就升格成为系统管理员了,到处指指点点,俨然一副资深管理员的样子,每次看到我再看计算机的书都会鄙夷的发出一声冷笑,然后和这些大妈一起,开始在背后嘀咕着揶揄我,什么大学生,咋没工作当打工的出纳了,这么用功装谁看啊,会打几个字真以为自己是计算机高手了之类的话.

我那时候也比较气盛,就想给他们点厉害看看,我就想破破这个司机的密码试试.银行这个系统用的是NETWARE的终端模式,程序是采用FOXPRO开发的,用户一登录后就通过PROFILE启动进入银行柜员程序,但是当时没有什么安全考虑,居然没有屏蔽CTRL-BREAK.于是在程序进入之前按下CTRL-BREAK.中断银行柜员程序，我轻易就进入到了DOS命令行模式,就可以直接用TYPE命令看到一些数据库DBF文件的内部信息了,包括用户的信息库.这个系统的用户密码是用程序加密过的,但是是程序员自己写的一个算法实现的加密,于是我通过不断修改自己的口令观看自己密文变化的方法,居然把这个算法给推导出来了.于是我破解计算出了这个司机也就是管理员的口令.当然我破解出来后什么也没做,毕竟我只是赌口气,没想过去干什么犯法的事,不过我在纸上写写画画计算算法和口令

的行为,被后面高度警惕的一干大妈时刻关注着.中午乘我吃饭的时候,她们把这张纸翻了出来,虽然她们看不懂写的什么,但她们拥有的特工一样高度敏锐的嗅觉还是告诉她们,此事不同寻常,于是她们拿着它集体去向社长报告我的异动行为,社长也不知道纸上我写的是什么,于是把信用社唯一的半IT人士,也就是这个司机兼系统管理员叫来让他分析,他虽然也看不懂,但最后一行是计算出来的他的密码他还是认识的,于是晚上,社长一行人到达了我家,鉴于我没有任何违法行为,但确实又破了管理员的口令,所以社长劝我主动辞职,理由是我太危险了,他在银行系统这么多年还没听说过出纳能破管理员密码的事情,他们担不起有我这样能力人在信用社工作的风险.于是2个月的信用社出纳的职业生涯,又到此为止.我的妈妈本来想埋怨我几句,但是被我父亲阻止住了,他只说了一句:“我的儿子肯定有前途,社长都说了,他在银行系统几十年都没听说过能破管理员密码的事情,但我儿子才学计算机几个月就能破,只要他不犯法,就说明了他有天赋”.我的父亲是一个严厉的父亲,从小到大,我挨他的打不计其数,记忆最深的两次,一次是我被父亲用荆棘条抽的混身是血道,让我表妹看到都吓哭了,还有一次是我高中在街上的棋摊上下围棋被我父亲看到直接在众人面前一顿猛抽嘴巴.但这一次却让我深刻感觉到了父亲的爱.当然我也深刻反省到,在职场上有职场的规矩,虽然我无犯罪之心,但是行为上确实触犯了很多规章与制度,也必须承担相应的后果.信用社这么处理我,是我完全应得的.

0x05 四处打工之寿险出单员(1997-1998)

丢了信用社的工作,我又处于失业状态.这个时候正好是寿险在国内开始开展的时候,加入寿险销售没有任何要求,当然收入也是全靠提成.于是我成了太保寿险的一名推销人员,做过简单的寿险业务培训后,然后就是开晨会搞激励,穿得笔挺上街做陌生拜访.加入寿险销售的一般以女性为主,男性不多,基本都是三十多岁以上,像我这样年纪的小伙没几个.我对业务的理解还凑合,但真到对人忽悠买保险就完全没路了.其他卖保险的都在忽悠客户若干年后能赚多少钱,如何比存银行划算,其实保监会都规定了寿险精算后的收益率是不能超过银行的利率的.保险保险,就是要降低风险而不是追求收益.但是国人对风险和安全的认识比不过对现实的利益追求,于是鼓吹自己的险种怎么比存银行能赢利倒成了国内推销保险的特色.自然我这种只会从降低风险角度去说服客人的销售业绩是一塌糊涂,不过业绩不好只是你拿不到提成而已,也没什么人来管我.

这个时候,保险也开始要求用电脑出单了,总公司下发了单机版的寿险出单程序,各地都要上.自然我们这也需要招一个会打字的寿险出单员,这个工作是聘用的,有400块固定工资,当时的经理为了刺激业务人员的积极性,于是规定,最近3个月业务成绩第一的人就可以获得这个职位,不过要自己学好打字,于是一帮人除了做业务外还开始学起打字来,热火朝天,虎视眈眈想拿到这份工作.当时保险行业延续了金融行业的惯例,这套程序使用的系统是SCOUNIX的,在哪个我们这会打字的人都比较少的年代,除了银行系统会这个的就更少了,不过经理也不懂,觉得能打字的就差不多可以出单了.我打字和折腾SCOUNIX固然没问题,但是推销寿险业务想要拿第一当然是天方夜潭了.我母亲知道后,于是开始为我到处跑业务,先我父母,我姐姐,我侄女,我亲戚什么的,全部被我母亲动员买了保险.然后我母亲带着我一个熟人一个熟人去拜访卖保险,靠着我母亲的面子,我终于成了这3个月寿险销售的第一名.如愿以偿地拿到这份工作,一个寿险出单员.

寿险出单对我来说轻而易举.我们是州府,下面还辖着的8个县市按要求也必须电脑出单,当时下面会打字维护系统的人就更没有了,而且下面业务量也不大,配专有人员成本还是很高.于是老总让下面地市的人出差时带保单过来到我们这边出单,时效比较慢,保户意见也很大.于是我建议用传真的方式加快出单(那个时候用传真在我们这个偏远地带还是少量单位的事),于是老总让我出差去采购多台传真设备回来再教导地市的人使用.我怀揣着2万巨款到了武汉,找好了卖设备的人,谈好价格;第二天下午5点多我去提货,武汉电脑街这个时候居然空荡荡的,的士司机给我停远了200米多,我下车走过去的时候,居然被一群混混给围住了,先是逼我买光盘,后面就直接上来开始搜我身,买设备的钱放在一个比较脏的纸袋里拎着,要是给这帮人抢走了,我可赔不起.我一个激灵,于是主动用江湖口吻说道:兄弟,大家都是出来混生活的,我身上就200块钱.我主动把衣服口袋里的荷包都翻出来给他们看,确实只有我自

己用于零用的200块钱,我接着说到:大家出来都不容易,这100块请大家去买包烟抽,剩余的100,大家帮忙下,我多少要留点路费,谢谢各位兄弟手下留情.那些人看我好象确实也没什么钱的样子,领头的接过了钱,马上就四下散了.我才有惊无险地走到卖传真机的店里.

传真买回来之后,各县市的工作效率明显提高,老总也得到了上级的表扬,于是开始比较看重我,让我全权负责这套系统.寿险这套系统,是SCOUNIX+FOXPRO开发的,程序还是第一个版本,错误百出.地市级的公司根本没有维护能力.于是省级公司电脑部的人就疲于奔命在各地维护这套程序,而我们这里,是他们最畏惧来的地,97年春节,2天翻了3辆大客车,死亡100多号人,上了焦点访谈;但是一年多来,我们这边居然没叫他们来维护过,而一些程序的BUG,都需要他们去各地升级程序,而我们这里也没有让他们来升级过,他们感觉很不放心,担心我们这里在玩什么花招.于是武汉分公司电脑部的人决定过来做突击检查,他们来了之后,抽查了保单和统计数据,发现都正确无误.而那些需要修改程序的BUG,也都被我改过来了,他们这才知道我的存在.武汉分公司电脑部正为缺少人到处去跑各地维护程序着急,于是很自然,我被抽调到武汉分公司电脑部.终于,我由一个非IT专业人士,终于成了一个专职的IT人士.另外,我参加了98年的水平高级程序员的考试,我早早第一个做完了试卷,本地的监考老师显然很希望我们这里多出点成绩,因为之前我们这里还没有出一个高级程序员,看着后面急头搔耳的考生,于是拿着我的试卷让后面一干人等抄袭,抄完之后还给了我,我做了下检查,发现了一个错误,于是修正后交卷.

0x06 四处打工之水平高级程序员(1998-1999)

太保武汉电脑部我没呆多长时间,工资是550,涨了一些,但是武汉的生活成本更高.而且显然,这里也很难转成正式的职位.我的父母一直希望我能找一个稳定的工作,也希望我能呆在家乡,他们通过关系找到本地一所大学的校长,让我去这所学校当老师,校长答应呆到一定时间后可以转正,于是我又回来成了该学校的一个编外计算机老师,职责是管一个小机房,10来台机器,专门给老师上网用的.

我97年就初次接触了互联网,买传真机时对方送了一张瀛海威免费几个小时的光盘,但是需要长途电话到北京,上网免费但是电话费得自己出.回来后我偷偷上去了几次,第一次认识到互联网,不过当月老总就抱怨电话费过高,要查查,之后就不敢多做这样高花消的事情了.98年,我高中同学在华中理工大学读博,去他们学校上了下教育网,见到的就更多了,BBS,TELNET,都是我以前没有见到的新奇玩意.这个时候,电信也开始有了互联网业务,我们那出现了第一个网吧,价格是10块钱1小时,我每个星期会去奢侈1个小时.各地电信开始纷纷建各种在线的站点,也有了聊天室这样互动的应用,我经常去的一个聊天室,我发现它注册的聊天室用户都是写在一个文本文件里,用||分割开,里面包含描述用户权限的信息,标记是管理员还是普通用户,但是没有对用户注册时的||做过滤.于是我注册用户时,使用||字符,后面就可以再增加一个管理员权限帐户,原理类似SQL注射,于是就成了这个聊天室的管理员.于是在里面踢踢人,偷看偷看聊天记录什么的.

这个学校的计算机系是由数学系分出来刚成立的,上课老师都是以前数学系毕业后留校的老师.学生学习热情很高,但感觉学不到东西,这个系的学生会主席不知怎么就打听到我对互联网了解很多(其实当时我也只懂得点皮毛),于是找到我,希望我能给同学办一次讲座讲讲互联网知识,我欣然答应了.讲座很快就开了,学生爆满.当时我讲的主要就是利用HTML和脚本编程可以做个简单的聊天室应用,这在现在是很平常的东西,但在那时和我们那里,确实非常超前和震撼的东西,讲座举办的非常成功,但是很多编制内的老师,对我则非常不满,在他们看来,我只是一个打杂的(除了管这个小机房,系里打杂的事也归我做),居然也敢办讲座.
在老师上机的机器上,我给几台机器安装了SCOUNIX+WINDOWS的双系统环境,一方面便我继续玩UNIX系统,另一方面,学校教操作系统课程也是以UNIX为典范的.给老师提供UNIX使用环境在我看来并没什么问题,但是却没想到出现了一个意外.一天一位教操作系统的老师来上机,我自然让他坐到装了双系统的主机上.过了一会,他脸色铁青的关掉电源就走了,我也没注意.过了2天一个和我关系还不错的老师跑来对我说:你有大麻烦了,系里所有老师在开会申讨你.我奇怪问为什么?他说,因为教操作系统的老师说你改了CMOS开机密码,故意阻碍老师上机,我一

晕,这那跟那啊?想起来了,双系统起来时候,是在BOOT界面上,直接按回车进入UNIX,敲DOS进入WINDOWS,用过UNIX的人都知道,但是我却从来没有想到过,专门教学生UNIX的老师居然从来没见过用过UNIX,不知道这是什么,还误以为我给他们上密码.

晚上系主任找我谈话,不外乎就是我锋芒太露,我们专职老师都不敢给学生办讲座.你凭什么办?你是有关系通过校长到我们这里来的,但也得本份之类的话.我对系主任说:我辞职好了,然后走出了系主任的办公室,我又失去了一份工作.

之后,我去了本地一家卖财会电算化软件和培训使用,顺带做一些硬件维护的公司,给人拆机换配件,装系统,扛机器是我这段时期做的最多的工作,除此外就是继续去网吧,99年大使馆被炸后引起了国内第一次有组织的黑客行为,我那时候对安全不太了解,但是凭着对UNIX的一些了解,居然也误打误猜到一台UNIX主机的口令,不过进去转了一圈也就出来了.很快这家财会电算化公司就不满意我了,毕竟我拆卸和扛机器的速度不咋滴,我很识趣就自己辞职了;几年后,我的一位若干年没见面的初中同学后来成为这家公司的技术主管,偶然碰到我问起我,惊奇地得知我曾在这家公司工作过,于是去找几位还留在该公司的老人问对我的影响如何,他们鄙夷的说了一声:技术非常烂,给机器换个配件都要10分钟.

就在我生命又一次暗淡的时候,终于出现了一线转机,我98年考的水平高级程序员的成绩终于出来了,我以高分过了,是那年我们州里唯一过的高程.主管程序员考试的人告诉我,由于监考老师当时把我的卷子给别人抄袭,导致我们这次州有多个高分过线的,答案又明显一致,而且我们历年没有过水平高的人,所以当时决定全部做作废处理,但是一位改卷老师说肯定有一个是原始被抄的人,而且这个地方这么落后好不容易出一个高程,还是应该照顾下,最后由于我分数比别人高半分,而且明显是改了一个错误点,说明我是原始被抄的.于是就批了让我一个过.虽然我不知真假,如果是真的,我想我要感谢这位不知名的老师,是他的一念之仁,给了我机会.

有了水平高级程序员的证书,我这个非计算机专业毕业的半路和尚,第一次拥有了一个能证明自己能力的证书了,于是我又花了口袋里不多的10元钱去网吧上网,在刚开始出现的一些招聘网站上,四处投放简历,简历上我加上了一行字:1998年水平高级程序员.

0x07 职业IT生涯之DELPHI程序员(1999-2000)

很快,X州的一家L公司打电话过来,对我进行面试.他们开发用的是PASCAL语言为基础的DELPHI开发环境.他们希望我能很快上手干活,除了一些计算机系统方面的问题,所以也问了一些DELPHI开发的问题,我只自学过C和FORTRAN语言,对这些问题只能依靠理解蒙混着回答,其实当时我不是很了解这些问题的正确答案,但很显然我运气不错,他们对我的回答很满意,电话里就决定录用我,工资是2000多;从500多一下飞跃到2000多多,这对当时的我来说简直是意想不到的工资;对方要我尽快就到岗,于是二话不说,买了次日去武汉的汽车,但是DELPHI还得靠临时抱佛脚,本地没什么卖计算机书籍的地方,只能到了武汉后,买了晚点去X州的火车票,马上就去书店买了2本DELPHI开发的书;我不想失去这份工作,他们以为我以前做过DELPHI开发才录用我的,我必须要利用在火车上的不到2天的时间成为能用DELPHI编程的人,千万不能让自己露陷;对于一个长期每个月拿4、500工资甚至经常失业在家吃父母白饭的人,2000多的工资实在是太有诱惑力了,而且这是第一份我凭自己本事找到的工作.

到达X州L公司时已经是下午三四点多了,显然不可能在这个时候就安排我开始干活,我庆幸又多了一个晚上可以突击学DELPHI,晚上安排好住宿后买了点物品,又温习了一遍DELPHI的东西才睡觉.但心里还是没谱,毕竟,连DELPHI都还没有安装使用过一次.第二天,公司给安排好了工作机器,接手一个调走到其他岗位的程序员的工作,学会安装好DELPHI,开始上手干活了,我一边靠临时背的点知识,一边看人家的代码和DELPHI里的开发指南帮助,开始了第一天职业程序员的生涯.

一个星期下来,我差不多能熟练使用DELPHI进行程序开发,除了一些比较深入的东西还需要时间掌握外,应付些日常的问题已经差不多.也开始了解到L公司更多的一些信息,L公司是科大毕业的6个人合伙创办的一家公司,负责技术也就是面试我的是科大少年班出来的,当时任总工.才17岁,但已经非常老成了.这家公司主要以开发医院的HIS系统为主,他们当时拿到了X州医院的一个HIS项目,然后又拿到一个X州本地老板200万投资,在这家公司我也接触更多的如QQ,新浪这些新生的互联网事务;显然他们也感觉到了互联网这个潮流,在总工的力主下,还在做一个网上商城的站点,他们做网上商城是非常早的了,如真能坚持到现在,没准成功的就是他们.但他们除了网上商城的商业模式外,显然还面临另一个更严重的问题,他们6个人,每个人单纯论个人技术都是很不错的,但在一起就有点谁也不太服谁的样子,经常争吵不休;我没搞懂当年他们是怎么凑到一起来创业的,也不太清楚他们的股权分配情况和决策体系.但是能看到CEO的职位老是走马灯式的换,每个人当1,2个月,然后就会在吵闹中换另一个人上来当CEO.所以在方向上也是变化不定,不过他们变化快倒逼着我学到不少新的东西,他们要做商城,我学JS,HTML,ASP这些WEB开发,他们决定做网上诊断系统,我学XML的应用,他们决定做餐饮和酒店系统,于是我又成了系统分析员和架构设计师.另外就是公司有一个喜欢玩黑客攻击的姓许的同事,经常拿一些发布的安全漏洞的攻击程序黑同事的机器来恶作剧,我也被他黑过一次,算是个小插曲.

但是渐渐的,我开始觉得公司问题越来越大了,技术创业型公司不擅长市场和营销的特性显得突出起来,HIS系统没有拿到新的单子,餐馆和酒店系统也只卖出去几套.商城也没找来投资或者形成一种赚钱的商业模式,对一个创业公司来说可能负担就比较重了,这个商城是总工力排众议要做的,但是随着时间推移压力逐步增大,内部争吵也越来越激烈.虽然后面又拿到老板追加的100万投资,但公司的方向好象就从来没有稳定过,在各种不同的方向中摇摆着,天天几大巨头都为各种决策吵闹不休,甚至出现了动拳头的事件,让下面的人也人心惶惶起来.后面一些开发主力也开始辞职了,特别是一位也是科大毕业,主要负责HIS架构的人员也离职了,他是当时公司除了总工外技术上最核心的人员,让我开始隐隐有所担心.我想,或许该考虑换换了.正好这个时候,一位先离职去了S市的同事打电话来,说他在S市找到了一个有钱的大佬,愿意投资他做套进销存软件.大佬把办公室都已经租好了,让我赶紧去S市和他一起图谋发展,大展拳脚,许诺给我的工资是4000.看来是该去有名的改革开放之地S市见识见识改革开放的成效了.

0x08 职业IT生涯之WEB程序员(2000-2001)

来到了S市,见到了这位朋友,然后接触到这个愿意投资的大佬,就开始发现这件事情很不靠谱.原来这个大佬是个爆发户,他的职业是某证券公司的投资经理之类的,那几年正是国内股市大发展的时代,他通过自己私人募集了一些资金跟着所在的证券公司一起炒股,赚了几千万,就开始想做点实业.不知被什么人教唆,说做软件公司赚钱快,做完了之后就可以在家等着数钱,举的例子就是广州某市一家做财会软件的公司,做了套财务软件,一年赚了好几个亿;因此他的计划是我们这个进销存软件一个月之内就要出来,他就好开始等着在家收钱了;大佬讲到这里,已经眉飞色舞,好象已经看见钞票在向他招手,这不扯淡嘛.软件一行代码都还没写就等收钱,就算我们能一个月做出来,你的销售,渠道和市场推广计划这些东西,这位大佬也好象没有什么想法和准备,于是我就给这位大佬解释软件的开发过程,说不可能这么快就出来,而且建设销售渠道这些事也不是几个月就能搞定的事.看着这位大佬幻灭的眼神,才知道破人发财的梦想实在是一件很得罪人的事情.不过大佬就是大佬,立马当机立断就做出了新的决策:既然做软件赚钱这么慢这么难,那我还是继续做我老本行证券相关的业务划算,原来注册为XX软件公司的办公室,立刻改头换面成为XX理财公司的办公室,于是我又要去找工作了.

幸运的是,凭着懂得一些WEB的编程知识和高程的证书,很快找到了一家马来西亚在S市做在线酒店订房和旅游推广的互联网公司,他们正好需要在WEB上做XML相关开发的人,于是我顺利的进去.在这里我认识了喜欢折腾LINUX和安全的DXK,那几年,以民族口号为诉求的各类XX黑客行动正如火如荼,DXk也经常去参与一下,因此也认识了不少做安全的人,我最早认识的一批做安全的人都是他介绍给我认识的,包括小鱼巫师,冰河,SSQ,苏樱等.

在DXK的带动下,我第一次学会了利用安全漏洞和相关利用工具.学会了拿着扫描器去扫描扫描主机和对一些常见工具的使用方法,不过也都只是玩玩而已.在这家公司另外的一个成就就是,当年IBM的DB2刚刚进入国内,为了推广DB2以及相关的认证考试,于是展开了网上在线的DB2的认证考试,考过之后可以获得DB2的各项认证,包括DB2的DBA,DB2的程序开发和高级程序开发三个认证.DXK是一直搞DB2的,我只是跟着他混混了解了些DB2DBA的皮毛.所以DXK就兴冲冲去网上考了下,但是没有过,回头对我抱怨题目比较难.我于是上去,找了个这个考试程序的BUG,轻易获得了这些题目的正确答案,于是这三个考试我都顺利拿到了100分,回来悄悄告诉了DXK,我们两都顺利地拿到DB2的这个3个认证.

不过很快,轰轰烈烈的互联网泡沫开始破灭,这个互联网公司也受到很大的冲击.开始收缩裁员,控制费用,马来西亚籍的CTO找我和DXK谈了2次话,希望我们继续留下,但很显然,公司好象很难继续维持下去了,他们开始找各种人来接手,最后找到了一个日本人来收购,我不太喜欢未来是被日本人管着,于是开始在网上投寄简历.寻找下一份工作.

不久,就有家M公司回复,让我去面试.我来到M公司,见到了负责研发的K总,相谈甚欢.于是就定下了去这家公司.

我新来到的这家M公司,是S市的一个民营企业,老板姓W,有点传奇色彩,传说他当年只身来到S市打工,在一个综合布线做机房工程的公司做仓管,一天客户来了,所有销售人员都外出了所以没有人员接待客户,他主动跳出来给客户讲解产品,让客户很满意,最后达成了交易,老板知道后非常惊奇,于是升他做销售,一年后就成了该公司的销售主管.后来他的客户关系多了,就私下接了一个大单,然后自己带领了几个弟弟,亲戚之类的单独做,几年时间内已经做到年销售5000万左右,是一个典型的家族公司.他的名言就是只要你给我做出块砖头我就能给你卖掉.M公司在证券行业做机房集成工程是非常有名的,但是利润则随着行业的规范化发展则变薄.因此W老板希望能跨向利润率更高的软件行业发展,于是挖来了K总,设立了软件研发部门,开始招兵买马.就是在这个背景之下,我来到了M公司.

0x09 职业IT生涯之开放式基金(2001-2002)

K总以前是某证券公司的技术部门经理,自己工作之外还开发了一套针对证券部门进行监管的软件，也希望能推向市场。K总有开发能力,管理经验，又有成型产品，证券行业背景。W老板有平台，有资源，自然是一拍既合，K总带产品加入，成了M公司的小股东兼副总裁，主要负责研发。

当时W老板拿到了某知名基金公司的开放式基金交易系统的开发和集成的单子，带设备和软件开发，项目金额接近2千万。我是K总招来的第三位研发类员工，不过第一位员工很快就自己闪了，第二位是一个女孩，于是我就自然成为了这个项目的项目经理，实际也是开发部门的经理，负责这个开放式基金系统的开发。那时候开放式基金在国内刚起步，证监会只出台了一个模糊的文件，具体业务规则该怎么做，就得基金公司和开发商自己去慢慢琢磨了，我当时面临最大的问题第一个是技术问题第二个是业务问题，技术上，这套系统使用的是IBMRS6000的小型机，AIX操作系统,对方要求是沿袭金融体系的那一套复杂的架构，使用CICS,tuxedo的中间件，MQ的消息中间件，除了DB2数据库外，这些技术都是我以前没有遇到过的，陆续招进来的人也没用过的，我只能天天捧着技术文档，从装AIX系统开始，配置各种系统的参数，一个一个的来解决，终于把整个系统架起来，能在TUXEDO,MQ下做开发，调试各种中间件的代码了。业务是另一个难题，开放式基金在世界上有2套差异很大的规则，一套是日本规则，一套是欧美规则，证监会的文件上并没说使用那家的规则，我们只能两个规则对照着研究，结合证监会文件一个字一个字扣字眼，看那种规则更符合文件精神。这样下来，我们开发组的成员个个都几乎成了开放式基金的业务专家（后来我的这些同事基本都去了甲方当技术经理了）。

做完了这个项目，W老板又折腾到和另一个基金公司谈开放式基金项目的机会。业务和技术都由我去谈，那时候我还对商业礼貌没什么观念，因为大夏天，我就穿了个大短裤和拖鞋去客户那里谈。由于业务和技术解说上都让对方很满意，对方立马就拍板了这个项目，理由是，穿了个大短裤和拖鞋的我，让他们觉得我们是做技术

而不是专忽悠的公司。只是这个项目比以前那个项目总金额少多了，800万。因为换成HP的小型机了，基金行业逐步认识到，其实开放式基金的交易量不可能如以前想象的象证券交易那么大，主要的计算只在每天下班之后的清算上，对实时性要求并不高，并不需要非常高端的设备才能完成。

这个时候我和K总发生了一些分歧，一个是对一些人的看法，公司软件业务发展后新成立了一些部门，进了一些经理，有些人做事我比较看不惯。但却成为了K总的心腹。其中我部门有一个湖南的漂亮小女孩做美工，对她垂涎的人不少。有一个部门经理和别人打赌要泡这个女孩，然后就对她非常殷勤，我曾经对这个女孩暗示过这个人不可信，但她却被爱情冲昏了头脑，觉得这个人就是她的真爱，而且这人还暗示他家有背景，拿钱在S市开了一家酒吧，她更陷入到做酒吧老板娘的虚荣美梦中，觉得一切说他不好的人都是嫉妒他。我本来是想把她介绍给我手下一个稳重老实的湖南程序员的，也只能做罢。这个经理心机很重，为了怕后面在公司有不好的影响，就劝这个女孩辞职找其他的工作。理由是，2个人在一家公司工作谈恋爱不方便，于是这女孩还真傻乎乎辞了这边的工作，找了个房地产销售的工作。后来那人终于得手，玩了一个月后就把她甩了。她去酒吧找这人，被赶了出来，之后她就天天都去一些各种酒吧泡着，希望能遇见更有钱的人把面子找回来。（这些都是后来和他打赌的人说出来的。我离开S市后听别人说，这个女孩子运气好，在酒吧碰到一个真心喜欢她的人，多次在她酒醉之后保护了她，最后终于走到了一起，后来生了孩子，安心做了家庭主妇，悲剧才没继续）。一个就是号称很懂安全的，把M公司网站黑了然后以此来自我推荐的人，一见面就号称自己认识这个安全圈牛人那个安全圈牛人，当时投了我这边的简历我来面的,觉得言过其实，就拒了。他同时又投了上面那位经理的职位，上面那位经理向K总极力推荐，K总聊了之后对他也一见如故，立刻招了进来，任命为质检部的经理。本来我就和他不太对胃口，质检部和开发部之间业务关系上也是比较容易起冲突的，于是在工作中两个部门就有些针锋对麦芒的意思了。另一个就是对开放式基金系统市场未来发展的方向上，K总还沉浸在前几个项目一家几百万上千万的模式上，认为中国有几百家基金公司，每年我们能做5家就不得了。我直接反驳说，高利润必然引来更多竞争者，以前做证券交易系统的公司都会抢过来吃这块肉，价格竞争会更激烈，和他们比我们没优势。后来确实印证了我的看法，不到一年，由于各家做证券交易的公司杀入这个领域，开放式基金系统使用PC服务器逐步成为标配，由以前的上千万项目规模跌到最低不到一百万的规模上。

由于开发部门和质检部门的工作一直比较对立，K总和我谈了几次话，我就主动申请了靠边站，K总给我成立了一个新部门：系统策划部去当经理，不再过问开发事宜。主要是研究新系统和新方向，简单点说，就是K总以前带来的证券监控软件，希望增加一些新的功能，如SNMP监控和一些安全功能，然后向证券行业去推广。这个事，让我正式和安全开始结缘。另外就是在此期间认识了XFOCUS的BENJURYY等兄弟，以及SHOTGUN等人。

0x0a 安全研究生涯之转折(2002)

给这个软件完成了SNMP功能后，接着就是实现端口到进程的映射研究，让我和安全圈的朋友不打不相识。

端口到进程的映射关系，当时微软并没有公开的技术文档来说明。但是国外的一个软件FPORT却实现了这个功能。于是FPORT成为我第一个逆向研究的程序，花了大半个月，通过汇编代码分析逆向成伪代码，终于把整个FPORT的过程机制分析清楚了。那个时候经常去SHOTGUN当斑竹的西祠黑客也是侠的版面，看到很多人也在讨论这个问题，于是发布了我写的这个工具。那里知道却引起了一场风波，很多人上来骂我用别人的工具说成自己的工具，让我莫名其妙，最后才知道，原来白细胞的ilsy也写了个同样的工具发布了，而我消息比较闭塞，并不知道他的工作，所以大家都认为我是偷盗了他的成果忽悠成自己的东西。我自然不服气，于是把我写的源代码，FPORT机理的分析，以及我逆向分析了ilsy的工具之后得出的我们之间技术的区别贴在了论坛上。于是指责停止了，这让我感觉到，安全技术圈子的人还是很实在的，只要你能拿出证据来，人家就服你。也是从这次风波中，知道了XFOCUS站点，以前虽然认识BENJURRY和冰河，但不知道他们是XFOCUS的人。去

XFOCUS上看安全技术相关的文章让我收益匪浅，于是觉得自己也可以通过研究，写出一些文章来，于是就把自己对安全的一些研究心得和成果，写出来发布在XFOCUS上，以此认识了更多XFOCUS的核心成员，小呆、ISNO等，其中ISNO还给我了UNICODESHELL编码的例子，让我更深入理解了SHELLCODE的一些原理和技巧。

XFOCUS上发布的文章多了，自然也和XFOCUS的兄弟熟悉了，然后由BENJURRY和冰河做介绍人，我也就加入了XFOCUS,感觉安全给我打开了另外一扇窗户，而且这期间也发现了一些微软的安全漏洞，如管道匿名劫持，ODBC查找SQLSERVER存在堆栈溢出等，虽然将这些信息发给了微软也石沉大海，但对安全的研究兴趣也越来越浓。于是开始考虑是不是要转入安全领域，这一年我已经29岁了，即将而立。比我小很多的人，早已是安全领域知名的人物了。我擅长的应用开发系统分析，都将随这一选择全部被抛弃，进入一个陌生的领域，我能行吗？但我已深深被研究安全的乐趣所吸引。于是给几家大的安全公司，包括启明和绿盟都投过简历，但估计我以前没有安全行业经验，年纪也偏大，学历也不符合，所以基本没消息。

随着基金系统市场这块蛋糕减少，M公司内部也出现了很多分歧，当年老板找K总来成立研发中心是看中软件这块高利润蛋糕的，前面上千万的项目规模也让他对现在在竞争中开发式基金系统的价格如此跌价难以接受，软件开发这一块现在近4,50号人，但是收入却比以前要大幅萎缩。K总性格比较强势，以前软件业务很赚钱的时候，W老板能忍，但现在业务不好，W老板肯定希望做出很多调整，自然和K总的强势性格形成冲突。我预感到风雨既来，离开吧。正好冰河对我说北京LX安全事业部在招安全人员，他可以介绍我去，小榕也在那里。于是29岁生日那天，我正式向K总提出辞职，晚上和开发部门的兄弟告别，我喝了不少酒，就要离开自己一同成长起来的团队，心里也很难受。

说下K总，我一直很感激K总，他虽然性格比较强势，但确实是想做事也有能力做事的一个人，对我也很赏识，后来虽然和我意见不合，但基本都是明对明的。后来我还留在M公司的同事告诉我，K总最后和W老板闹翻，先是降级成部门经理，最后走人，而他一直器重的质检部经理。先后成了总监和总裁助理。03年底我接到过K总的电话问我怎样，听得出是想拉我再起炉灶，我当时在安全行业已经做出了些成绩站稳了脚跟，自然不会再折腾那个我已经放弃了的行业了。于是告诉他我很好。之后听说他做过很多行当，包括租虚拟办公室，再之后我在他BLOG上看到，全都是他拍摄的很专业的摄影照片，不知是他转成专职的摄影师还是就有爱好（这个爱好以前我没听说过）。后来，M公司软件部门大裁员，很多人都在公司红黑榜站点上大骂W老板心黑，没能力。我回复了一条："我算是老一批的M员工了，在M公司当开放式基金项目的项目经理以及以后的研究策划部的经理，2002年底觉得公司在软件上的发展存在问题,就离开了M，做安全去了。公正的讲，M存在很多问题，比如家族企业，内部互斗，但是这些问题在其他企业的身上也一样存在。我在M学到了很多东西（虽然这些随着我行业的转向现在完全没用了），或许我离开的时机还不错，离开半年后，我的股份后来还是给我兑成钱了。漫骂是没多少用的，企业的问题不能靠漫骂解决，如果看不上这个企业，就离开他好了。我还是很佩服W的，白手起家能折腾到这个规模还是非常不容易的。"

从M公司走时，我历年来的积蓄是5万，化了1万多买了个笔记本，来到北京，又租了个在LX安全事业部附近的房子，又花了几千买了西服等行头，准备去LX安全事业部应聘。但从应聘反馈回来的信息是：技术上我虽然没问题，但是学历是个麻烦，非计算机专业的专科，在LX这样的大公司里，必须要总裁特批才能进去。我问这个总裁特批需要多久呢，对方说，至少3个月以上吧。我看了看荷包里剩余不多的钞票，想想至少3个月，没准是半年一年呢，我这荷包可等不起，而且春节要来了，好歹要赚点车票钱和回家给小辈的压岁钱，看来只能另谋出路了。

0x0b 安全生涯之冲击波(2003)

于是，我来到A公司。A公司是一家在北京做安全的小公司，他们的总工一直和我在QQ上有联系，所以我很快就进去了，里面还有几个技术不错的人，其实我来这也就是混个过年，开年再想办法，其实我很感谢这位总工，很明显他也知道我的这种想法，知道我在A公司呆不长，但还是让我进去混了一个月的工资，春节放假时还给我发了1000块的红包。还破天荒带我去和YUANGE吃了个饭介绍了我一下，当时YUANGE已经是安全技术圈子里的神话，当然没有听说过我。所以后面就是总工和YUANGE在上面侃侃而谈，我就在下面大口吃肉。顺便提下YUANGE，YUANGE让我影响最深刻的一篇文章是02年就有一篇关于UNICODE短整数表示长度的方式会有可能触发溢出的文章。若干年之后，某个知名0DAY漏洞爆光，我马上就联想到了这篇文章，看来当年YUANGE写这篇文章时，很大可能就已经藏着了这个0DAY。

在A公司也杂七杂八做了一些活，这个时候，我开始通过汇编逆向加动态调试方式，分析了多个微软未公开的协议，如SQL的TDS的协议。另外就是首届XCON开了，我凑了个<溢出植入型的木马>做为议题，参加了XCON，这个想法其实我觉得还是非常有意思的，不过后来基本不碰木马的方向了，也就没怎么研究了。议题结束时候，有幸被WRANG3大牛问了几个尖锐的问题，仓促应对完狼狈下场。会上也认识了不少安全技术圈的人，还有ILSY，当然是相逢一笑泯恩仇。

混过了年，再回到北京，我先委托STARDUST帮我介绍去绿盟，不过很久也没回复。看看自己的口袋，也急了，这时STONE对我说可以介绍我去启明，于是我就来到了启明应聘。比想象中简单，很快我就进到启明的功防实验室。开始做漏洞分析的一些技术研究。当时分析了很多缺乏技术说明的漏洞公告，这个阶段，让我对安全漏洞机智和攻击手段有了更多了解。虽然接着就碰到了SARS，在家呆了很久，还是写了大量的漏洞机制分析发布在XFOCUS的内部论坛。7月份，微软的MS03-26漏洞公告通报RPCDCOM有严重的远程安全漏洞，当时所有的WINDOWS操作系统都受影响。鉴于此漏洞的严重程度，微软和发现此漏洞的LSD组织都不给出任何细节，这意味着安全厂商必须自己去分析安全漏洞机理。

当时还没有BINDIFF这样的工具，漏洞的分析和重现靠人工分析，所以当时漏洞补丁到分析出来的周期大致是20天以上。攻防实验室经理的蔡晶晶对我说，赶快去分析吧，这可能是WINDOWS历史上最严重的安全漏洞。于是我开始了独自的分析和调试，3天后，发现了一个新的RPC拒绝服务漏洞，5，6天后终于再现了这个漏洞。漏洞分析文章写出来了。于是我找BENJURRY和XUNDI帮助翻译和增加了一些其他系统的JMPCODE，以XFOCUS的名义投寄到BUGTRAP上。我也没想到这一投寄，引起了很大的风浪，这是世界上第一个公布的该漏洞细节的文章，被美国的HDMORE修改后转载，很快在安全社区到处流传。由于那个时候绝大部分用户还没有打补丁的习惯。因此就意味着这个漏洞会影响当时很多WINDOWS系统，可能会形成蠕虫;微软立刻召开了记者会指责XFOCUS没有通知他们就发布了这篇文章。BUGTRAP上，全世界黑客都在用此文章给出的POC进行修改，验证。8月初，冲击波蠕虫如期而来，瞬间影响了上千万台主机，随后还有数十个蠕虫使用了这个漏洞，造成了巨大的损失，XFOCUS组织也被推到风口浪尖上。国内外的批评紧跟而来，我只接受了一个国内媒体的采访，阐述了我的看法:安全不是靠黑客不知道来保证的。这是一个针对已经修补的漏洞的技术分析文章，他不触犯任何法律和安全行业行规，因为漏洞已经被厂商修复，但是用户缺乏打补丁的意识导致的，降低用户损失的关键是教育用户及时打补丁。之后当BINDIFF这样的工具出现之后，重大漏洞从补丁到分析出来的时间周期已经缩短到3天，但用户打补丁的意识却被教育起来之后，安全损失则会大大降低。

当然冲击波事件，也让我开始正视，作为安全人员，一些行为确实可能会给用户带来危害。不可否认，我发布的POC被冲击波直接利用到冲击波代码里，虽然发布他们不违反法律和行规，但确实应该多考虑一下事件之后可能带来的损失。可以更加专业和职业一些，这是我在冲击波事件中学到的东西。

但无论如何，这篇技术分析文章让我正式成为一个被安全圈认可的安全研究人员，我以前的文章也开始被人关注。我2002年发现的2个微软的安全漏洞，当时由于给微软漏洞接收组发邮件，3个月都没收到回复，所以就公

布在了XFOCUS的文章里，也没什么人关注。但是冲击波后不久，我发现居然被国外一个安全研究组织一起上报给了微软并修复了。我虽然没有完全的证据，但猜测应该是看了我的文章，想到这些老外也得折腾看我们汉语写的文章，也算为汉语普及做了点贡献。冲击波事件里，我应该感激的人包括:蔡晶晶，启明的领导，BENJURRY和XUNDI，帮助我翻译，并增加了一些JMPCODE并发布到BUGTRAP上。XFOCUS的其他兄弟，在我遭受指责时和我共同承担了指责。

0x0c 安全生涯之冲击波(2003)

于是，我来到A公司。A公司是一家在北京做安全的小公司，他们的总工一直和我在QQ上有联系，所以我很快就进去了，里面还有几个技术不错的人，其实我来这也就是混个过年，开年再想办法，其实我很感谢这位总工，很明显他也知道我的这种想法，知道我在A公司呆不长，但还是让我进去混了一个月的工资，春节放假时还给我发了1000块的红包。还破天荒带我去和YUANGE吃了个饭介绍了我一下，当时YUANGE已经是安全技术圈子里的神话，当然没有听说过我。所以后面就是总工和YUANGE在上面侃侃而谈，我就在下面大口吃肉。顺便提下YUANGE，YUANGE让我影响最深刻的一篇文章是02年就有一篇关于UNICODE短整数表示长度的方式会有可能触发溢出的文章。若干年之后，某个知名0DAY漏洞爆光，我马上就联想到了这篇文章，看来当年YUANGE写这篇文章时，很大可能就已经藏着了这个0DAY。

在A公司也杂七杂八做了一些活，这个时候，我开始通过汇编逆向加动态调试方式，分析了多个微软未公开的协议，如SQL的TDS的协议。另外就是首届XCON开了，我凑了个<溢出植入型的木马>做为议题，参加了XCON，这个想法其实我觉得还是非常有意思的，不过后来基本不碰木马的方向了，也就没怎么研究了。议题结束时候，有幸被WRANG3大牛问了几个尖锐的问题，仓促应对完狼狈下场。会上也认识了不少安全技术圈的人，还有ILSY，当然是相逢一笑泯恩仇。

混过了年，再回到北京，我先委托STARDUST帮我介绍去绿盟，不过很久也没回复。看看自己的口袋，也急了，这时STONE对我说可以介绍我去启明，于是我就来到了启明应聘。比想象中简单，很快我就进到启明的功防实验室。开始做漏洞分析的一些技术研究。当时分析了很多缺乏技术说明的漏洞公告，这个阶段，让我对安全漏洞机智和攻击手段有了更多了解。虽然接着就碰到了SARS，在家呆了很久，还是写了大量的漏洞机制分析发布在XFOCUS的内部论坛。7月份，微软的MS03-26漏洞公告通报RPCDCOM有严重的远程安全漏洞，当时所有的WINDOWS操作系统都受影响。鉴于此漏洞的严重程度，微软和发现此漏洞的LSD组织都不给出任何细节，这意味着安全厂商必须自己去分析安全漏洞机理。

当时还没有BINDIFF这样的工具，漏洞的分析和重现靠人工分析，所以当时漏洞补丁到分析出来的周期大致是20天以上。攻防实验室经理的蔡晶晶对我说，赶快去分析吧，这可能是WINDOWS历史上最严重的安全漏洞。于是我开始了独自的分析和调试，3天后，发现了一个新的RPC拒绝服务漏洞，5，6天后终于再现了这个漏洞。漏洞分析文章写出来了。于是我找BENJURRY和XUNDI帮助翻译和增加了一些其他系统的JMPCODE，以XFOCUS的名义投寄到BUGTRAP上。我也没想到这一投寄，引起了很大的风浪，这是世界上第一个公布的该漏洞细节的文章，被美国的HDMORE修改后转载，很快在安全社区到处流传。由于那个时候绝大部分用户还没有打补丁的习惯。因此就意味着这个漏洞会影响当时很多WINDOWS系统，可能会形成蠕虫;微软立刻召开了记者会指责XFOCUS没有通知他们就发布了这篇文章。BUGTRAP上，全世界黑客都在用此文章给出的POC进行修改，验证。8月初，冲击波蠕虫如期而来，瞬间影响了上千万台主机，随后还有数十个蠕虫使用了这个漏洞，造成了巨大的损失，XFOCUS组织也被推到风口浪尖上。国内外的批评紧跟而来，我只接受了一个国内媒体的采访，阐述了我的看法:安全不是靠黑客不知道来保证的。这是一个针对已经修补的漏洞的技术分析文章，他不触犯任何法律和安全行业行规，因为漏洞已经被厂商修复，但是用户缺乏打补丁的意识导致的，降低用户

损失的关键是教育用户及时打补丁。之后当BINDIFF这样的工具出现之后，重大漏洞从补丁到分析出来的时间周期已经缩短到3天，但用户打补丁的意识却被教育起来之后，安全损失则会大大降低。

当然冲击波事件，也让我开始正视，作为安全人员，一些行为确实可能会给用户带来危害。不可否认，我发布的POC被冲击波直接利用到冲击波代码里，虽然发布他们不违反法律和行规，但确实应该多考虑一下事件之后可能带来的损失。可以更加专业和职业一些，这是我在冲击波事件中学到的东西。

但无论如何，这篇技术分析文章让我正式成为一个被安全圈认可的安全研究人员，我以前的文章也开始被人关注。我2002年发现的2个微软的安全漏洞，当时由于给微软漏洞接收组发邮件，3个月都没收到回复，所以就公布在了XFOCUS的文章里，也没什么人关注。但是冲击波后不久，我发现居然被国外一个安全研究组织一起上报给了微软并修复了。我虽然没有完全的证据，但猜测应该是看了我的文章，想到这些老外也得折腾看我们汉语写的文章，也算为汉语普及做了点贡献。冲击波事件里，我应该感激的人包括:蔡晶晶，启明的领导，BENJURRY和XUNDI，帮助我翻译，并增加了一些JMPCODE并发布到BUGTRAP上。XFOCUS的其他兄弟，在我遭受指责时和我共同承担了指责。

0x0d 安全生涯之新的研究(2003-2004)

2003-2004年研究的方向主要是一些系统机制与攻击利用技术上的研究。03年除了分析了WINDOWS认证过程与SMB协议外，主要的一个工作就是做了很多WINDOWS堆的分析。WINDOWS的堆除了前人分析出来的CHUNK结构和FREE链表外，整个堆的管理也是非常有趣的，如堆节的管理，扩展后的回调函数，堆块的融合过程，LOOKASIDE表。利用一些堆的特性，可以实现一些很难利用的堆溢出的利用，当初曾准备过一个议题，就是针对当时出的一个很难利用的堆溢出，利用堆的融合时的操作，巧妙的饶过这个限制实现利用，不过最后还是没找到合适的场合讲。之后，微软逐步增强了对堆上面的保护，WINDOWS2003SP1首次增加了链表一致性的检查。2003年的XCON，我的议题是《WINDOWS2003堆保护的饶过利用》就是针对当时WINDOWS2003SP1检查机制不完善，只针对摘链表做了检查，对插入链表没有做检查，攻击者可以伪造堆头构造释放，在插入链表时饶过保护。并且提出了将利用堆栈伪造符合条件的思路，可以将堆溢出转化为堆栈溢出的方式，之后沿着这条思路美国的MattConover(shok)找到了更好的方法，通过触发LOOKASIDE表使用形成天然的符合条件的方式，可以获取把任意内存当作一个堆CHUNK分配给用户任意使用来达到利用。MATT是安全领域的传奇少年，10几岁时就写出了的世界最早的堆溢出原理文章。在堆溢出领域研究非常深入。

2004年，我的研究重点先是转到WINDOWS内核远程溢出上，这一块以前全世界都没有人公开发布过相关的技术。正好赛门铁克的个人防火墙出了一个WINDOWS内核的远程溢出，之前我对内核也没什么接触，搞内核的溢出利用确实需要对内核很多机制有深入的了解，这一块，得到了科技师傅的大力帮助和支持，遇到对内核机制不了解的地方，科技就象一个活字典帮我解答一些疑难问题，终于成功实现了WINDOWS内核缓冲区远程溢出的稳定利用，在XCON上公布了WINDOWS内核远程利用的关键技巧但是没有公布代码。也被赛门铁克的报告里认为是世界上首个公布WINDOWS内核缓冲区远程溢出利用技术的演讲。这个演讲之后被SOBEIT分析研究做了改进公布出了代码。

这时我的兴趣逐步转向了漏洞挖掘，在这之前，漏洞挖掘基本靠人逆向分析源代码，比如yuange就是大家公认的肉眼挖掘机。2004年前我发现的几个安全漏洞都是靠很长时间协议分析和手动测试，逆向分析，花了很多时间才分析到，觉得这样找安全漏洞效率太低下。2003年SKIPE工具第一次把模糊FUZZ的思想引入了漏洞挖掘，取得了很不错的效果，但是SKIPE毕竟只是个简单的工具，还是很难有效去找更多安全漏洞。我当时就想，如果实现一个由异常监视，模糊器和自动化测试模块组成的框架，应该就能让测试程序自己去找安全漏洞，多配一些机器，找寻安全漏洞的效率会高很多。于是和科技师傅一起深入探讨了一些WINDOWS异常的表现，处理的机制等技术问题后，然后我写出了个原形展示给科技师傅看，科技也很感兴趣，又提出来可以做自动模拟键

盘和鼠标的功能，于是按照样本模糊器策略，异常监控，自动化实施组成的FUZZ框架很快成型，我和科技马上投入使用，效果非常显著，在我们测试的头两星期，就找到了一批微软产品的安全漏洞。于是我们整理出来3个，我发现的2个，科技发现的1个。发信给微软负责接收漏洞的邮箱。意料之中过了2周，没有任何响应，于是我们发布给漏洞公告的专业组织CVE，等CVE确认之后，这时微软还是没有什么响应就公布了出来。自然又引起了微软的一通公告式的指责。但我觉得作为我们安全厂商已经做到自己的义务了，主动联系你但你没响应，这样我们也是先提交CVE再公布的。后来当时的微软安全主管ANDREWCUSHMAN和我联系时又提及此事，我告诉他我们写了漏洞报告给微软，但是微软直到现在也没给我们回复过。他回去让人去查接受漏洞报告邮箱，果然找到了我们提交的报告，还没人打开阅读过。他向我表达了歉意并表示会整改此事，之后微软对来自中国的安全漏洞报告的响应速度就及时了很多。这几个漏洞中，值得一提的是ANI的整数溢出触发堆溢出的利用EXP，整数溢出触发堆溢出后由于拷贝的数据是整个表达范围的长度，注定都是会触发异常的，WINDOWS在堆栈之下可以利用SEH来在触发异常时获得控制权，但是在堆溢出中就缺乏这样的一个控制通道，而且堆被破坏之后很容易异常。但是在IE下面，攻击者存在很多可以控制堆内存布局的手段，这个就EXP就是生成多个HTML元素，利用HTML元素在堆上面的对象包含了大量函数指针，而且这些函数指针会被多线程例程调用，这样就有很大的几率在异常之前获得控制。这么多年来，微软产品的安全获得了足够的改进，但在IE上面，由于攻击者可以借力的渠道太多，而且大量流行的第三方的控件的机制和代码质量难以约束，IE的安全问题还是非常严峻。

0x0d 安全生涯之黑客游戏(2005)

随着我们公布安全漏洞的增加，我们关于漏洞挖掘的研究显然引起国际安全社区的注意，不久我就收到了美国知名安全公司EEYE首席技术官的邀请，让我去美国EEYE工作，在办好H1B签证之前可以在国内工作，待遇让我无法拒绝。当时我已经32岁，在启明的工作虽然很开心，启明的氛围不错，但是买房的压力也是相当的大。毕竟我已经不是21岁。

启明非常大度的让我离开了，回首在启明的日子，我是应该对启明抱有感恩之心的。在启明我成了一个真正的安全研究人员，启明里面的很多人传授给了我很多有用的经验和知识，帮助了我的成长，而启明管理者。至少对我，是非常宽容和大度的，虽然离开了启明，我还是要对他们真心说一声感谢。另外技术上对我帮助最大的是科技，说点科技的小八卦，他是一个不吃任何葱姜蒜辣椒等刺激品的人，他是舟山群岛的人，因为从小就不吃，所以非常敏感，有一次我在办公室吃一包花生，科技哥一脸严肃的走过来，要求我马上别吃了，因为花生里有大蒜的气味，他受不了。科技师傅还有很多怪习，比如不吃圆的物品，不吃面食。不过科技师傅在WINDOWS系统层的研究，确实非常深入，让我非常佩服，他至今还在启明。当然还有小波，村长等人，从他们那里我也学到不少东西。赵伟则帮助做了很多翻译的工作。另外，高端安全研究人员成为全球都比较紧缺的资源，在这之后，多家国际安全公司包括MCAFEE在内都在国内大举网罗高端的安全研究人员，毕竟他们可以用美国普通研究人员一半的薪水就能招到国内最顶尖的安全研究人员，比如MCAFEE挖走了小波，孙冰，SOBEIT;微软聘用了吴石和SOWHAT。基本上在XCON上作过PAPER的人，都会接到这些国外公司的OFFER。

EEYE那个时候在安全行业以漏洞挖掘和挂微软修补灯笼而闻名的一家美国公司，当时他的扫描器由于内嵌了能检测很多他们发现的但微软还没修复的安全漏洞而非常出名。他们还生产一些防火墙软件之类。我去之后主要的工作是帮助测试他们防火墙的安全和性能，不过所有研究团队的人，都有义务去找各种其他通用产品特别是微软的产品的高危安全漏洞，由EEYE报告给厂商，然后挂上灯笼。所谓灯笼就是报告厂商后，EEYE会出给公告，但不涉及到漏洞细节。根据厂商修复时间显示不同的警示信息，让很多修复时间长的厂商脸上不太挂得住。厂商修补出了补丁后，EEYE就会正式公告具体的漏洞细节和验证代码。

我还在国内办H1B签证，但给EEYE的工作已经开始了，CTO发了封邮件把我介绍给研究团队的成员，EEYE研究团队里有一群牛人，其中我最敬佩的是个美国研究员，发现了很多WINDOWS高危而且影响广的安全漏洞，我发现欧美的研究人员，一般对人比较友善，都主动发信给我过来致意。EEYE当时还有2个日本研究人员，当年做漏洞挖掘也很厉害，也爆了不少高危级的安全漏洞。其中一个还比较好，发了个邮件表示了下HELLO，另一个则明显不太友善，什么表示也没有。过了2天，CTO发邮件给我说，那个没表示的日本研究员希望和我做HACKGAME，就是比谁在最近几个月内，发现的安全漏洞越多，高危级越严重，谁就是胜利者，问我是否应战?我一笑接受了。

于是，我买了4，5台当时最高配置的机器，放在家里，每个机器上都开了多个虚拟机，除了给EEYE的产品做测试外，连天连夜用自己写的FUZZ工具去做漏洞挖掘。我是憋着一口气，所以一个个安全漏洞被找出来后，我马上加班加点做分析报告提交给EEYE，微软产品的，FLASH的，REALPLAY的，纷纷上了EEYE的灯笼榜，个数已经远远超过了EEYE的其他人，包括这个日本人;但我知道，不发现一个能通过常见服务远程利用的，理论上可以导致蠕虫级高危级的安全漏洞，这个日本人是不会服气的，于是又去测试一些系统默认会开启的RPC服务的进程，很快就找到了MSDTCRPC服务的高危级远程安全漏洞;不过这个漏洞按普通的理解是比较难利用的，但是我发现通过一些攻击技巧是可以实现非常稳定的利用。当这个漏洞提交上去后，这个日本人表示了下置疑，我早有准备，提交了稳定利用的SHELLCODE给EEYE，之后，再没听到这个日本人提起黑客游戏的话题了。

#渗透测试　　#传记

让你相见恨晚的python库　　上海地区 IT/互联网 大厂名录