IT热门：底层安全开发
BAT求职技巧

2015/06/16　麦洛克菲—周扬荣

麦洛克菲内核，底层，安全

www.mallocfree.com

报告提纲

- 底层安全技术介绍与演示
- BAT求职经验与技术
- 其他老师安全技术报告
- 礼物赠送：见者有份
- Q&A

安全技术现场演示

DEMO

IT热门领域--安全技术

- 安全很重要，谁也离不开“安全感”
- 属于底层技术，有技术壁垒，人才稀缺

名企对安全人才的需求

2014-02-25, 10:39:41 【招聘】畅游百万年薪诚聘顶级安全专家

公司名称：	北京畅游时代数码技术有限公司
职位名称：	游戏安全专家
招聘人数：	数人
工作地点：	北京市石景山区八角东街65号融科创意中心B座畅游大厦
薪水待遇：	顶级游戏安全专家 底薪50万，另有项目分成约50万

tombkeeper

“玄武实验室”是腾讯新成立的信息安全研究部门。无论擅长Windows、Linu
是Android、iOS，或任何其它你引以为傲的安全技术，如果有兴趣加入，i
历到：【xlab@tencent.com】。无论大学考上没考上毕业没毕业，还是博
士后博士左博士右，只看技术，不看文凭。工作地点在北京。

4分钟前 来自微博 weibo.com | 举报 (1) | 转发(7) | 收藏 |

公司名称：	奇虎360
职位名称：	病毒分析、后台驱动、数据挖掘、客户端开发
招聘人数：	若干
工作地点：	北京
薪水待遇：	15-40w年薪

2014-08-13, 12:07:07 【招聘】【阿里巴巴】招聘安全研发人才（长期有效）

公司名称：	阿里巴巴集团公司
职位名称：	安全资深研发高级工程师 / 安全研发专家/反病毒研发工程师/C、C++研发工程师
招聘人数：	长期招聘
工作地点：	杭州
薪水待遇：	5险1金，15-80k（待遇优厚）
职位描述：	安全相关产品的研发

公司名称：	百度
职位名称：	研发
招聘人数：	10
工作地点：	北京西二旗
薪水待遇：	15-25K
职位描述：	负责百度卫士百度杀毒的研发工作
联系人：	任梦

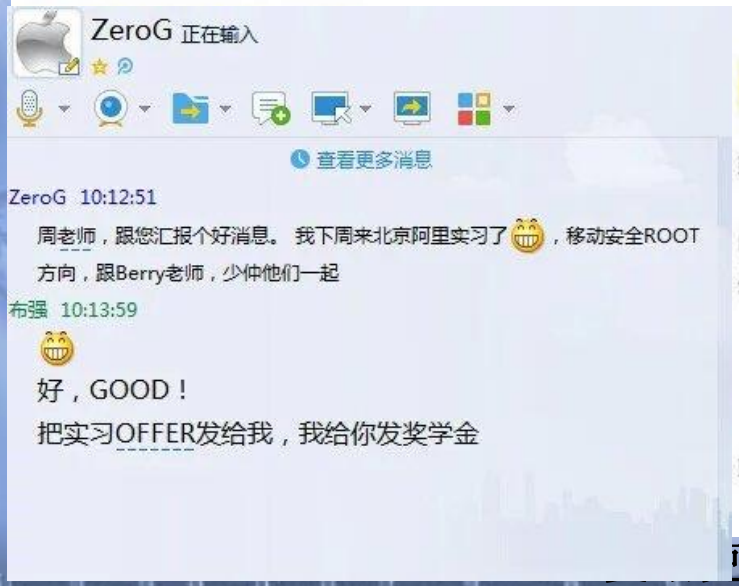
公司名称：	腾讯
职位名称：	漏洞安全研究员
招聘人数：	2
工作地点：	深圳
薪水待遇：	年薪20w~40w
职位描述：	负责Windows客户端、Android、Web等漏洞安全
联系人：	tobywu

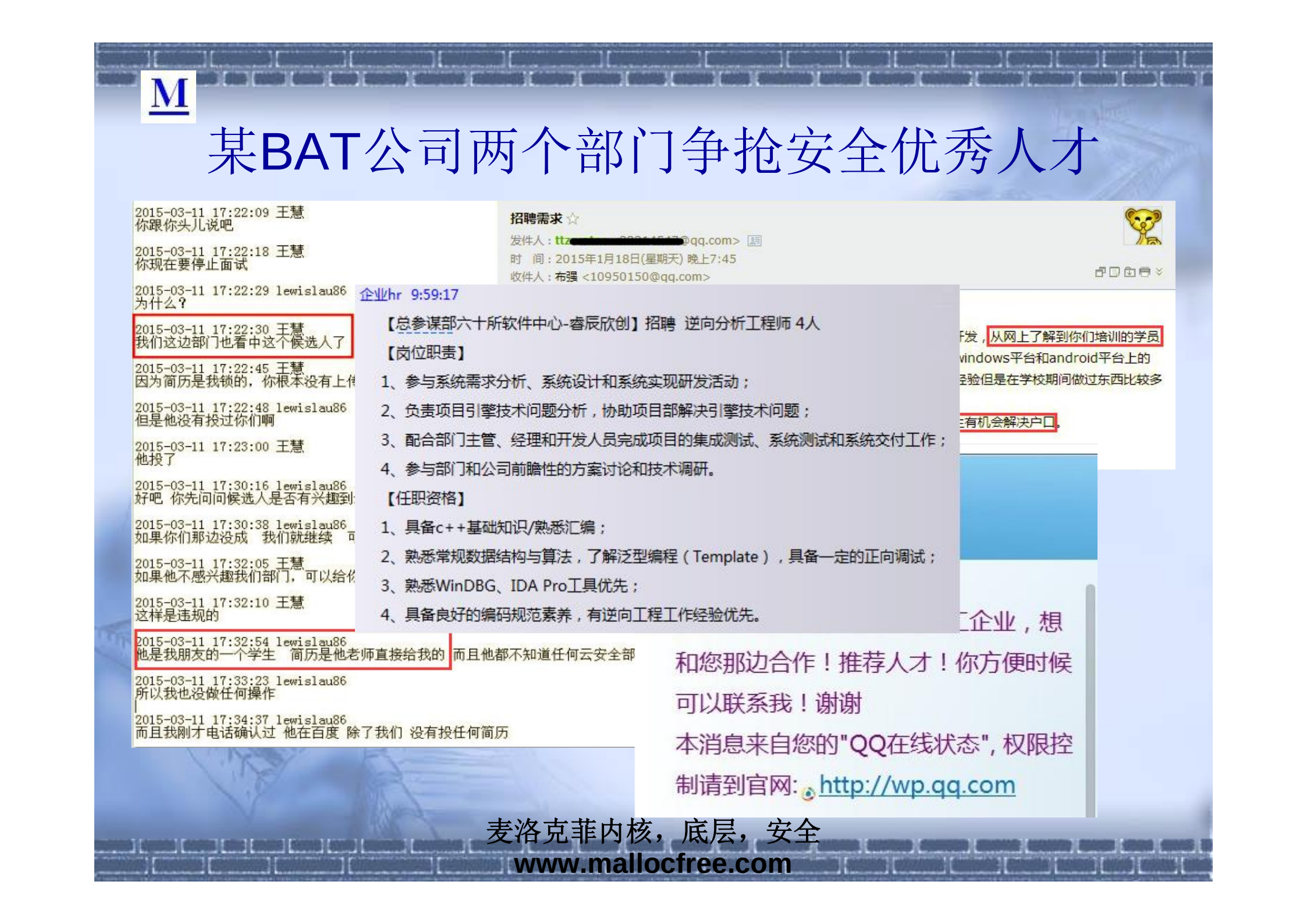
公司名称：	北京启明星辰信息技术有限公司
职位名称：	启明星辰安全开发工程师
招聘人数：	若干
工作地点：	北京市海淀区软件园三号路启明星辰大厦
薪水待遇：	6k-20k

麦洛克菲内核，底层，安全

www.mallocfree.com

部分名企OFFER-BAT，360



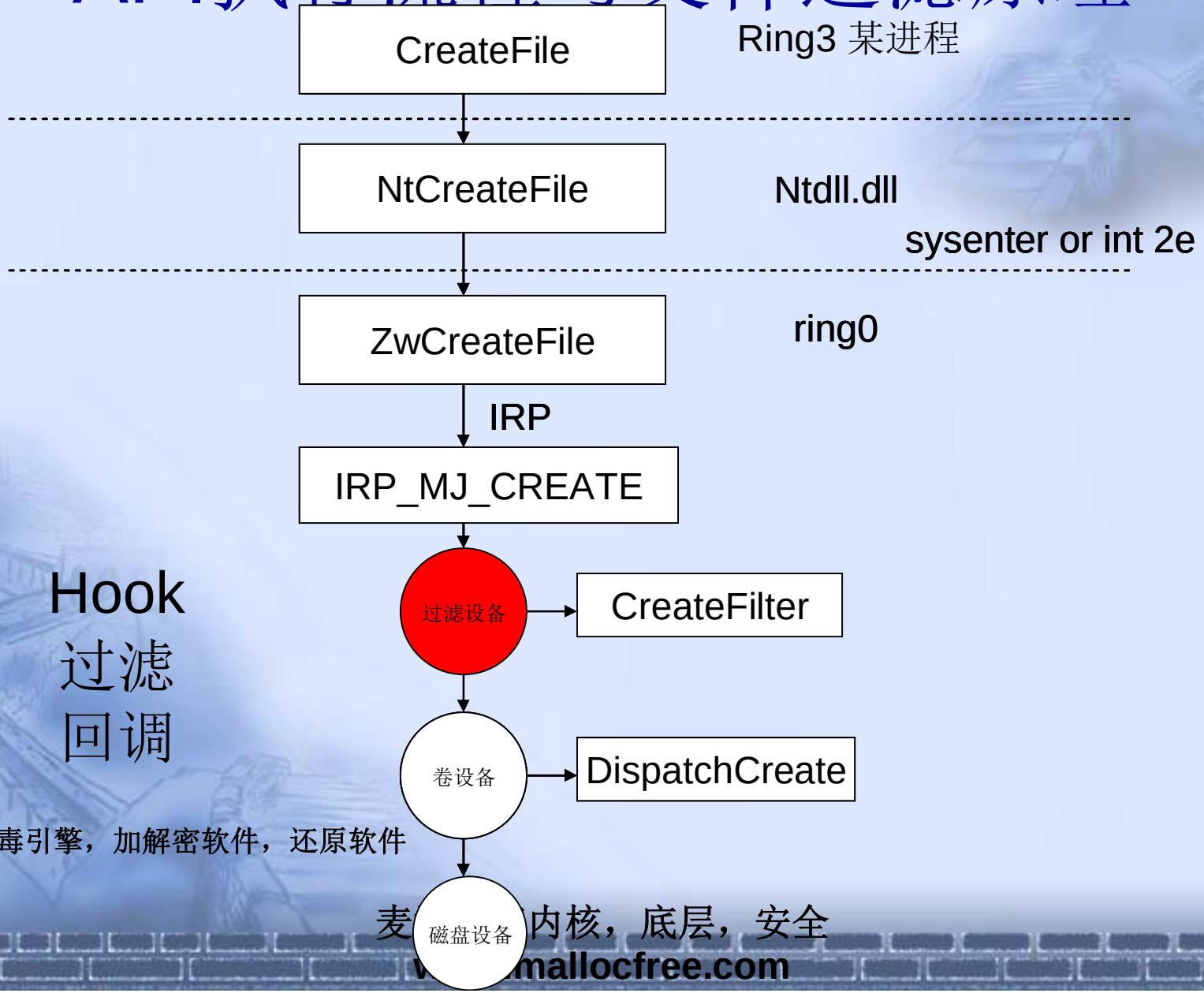

某BAT公司两个部门争抢安全优秀人才
2015-03-11 17:22:09 王慧
你跟你头儿说吧
2015-03-11 17:22:18 王慧
你现在要停止面试
2015-03-11 17:22:29 lewislau86
为什么？
2015-03-11 17:22:30 王慧
我们这边部门也看中这个候选人了
2015-03-11 17:22:45 王慧
因为简历是我锁的，你根本没有上
2015-03-11 17:22:48 lewislau86
但是他没有投过你们啊
2015-03-11 17:23:00 王慧
他投了
2015-03-11 17:30:16 lewislau86
好吧 你先问问候选人是否有兴趣到
2015-03-11 17:30:38 lewislau86
如果你们那边没成 我们就继续
2015-03-11 17:32:05 王慧
如果他不感兴趣我们部门，可以给
2015-03-11 17:32:10 王慧
这样是违规的
2015-03-11 17:32:54 lewislau86
他是我朋友的一个学生 简历是他老师直接给我的 而且他都不知道任何云安全部
2015-03-11 17:33:23 lewislau86
所以我也没做任何操作
2015-03-11 17:34:37 lewislau86
而且我刚才电话确认过 他在百度 除了我们 没有投任何简历
招聘需求
发件人：ttz[redacted]@qq.com>
时 间：2015年1月18日(星期天) 晚上7:45
收件人：布强 <10950150@qq.com>
企业hr 9:59:17
【总参谋部六十所软件中心-睿辰欣创】招聘 逆向分析工程师 4人
【岗位职责】
1、参与系统需求分析、系统设计和系统实现研发活动；
2、负责项目引擎技术问题分析，协助项目部解决引擎技术问题；
3、配合部门主管、经理和开发人员完成项目的集成测试、系统测试和系统交付工作；
4、参与部门和公司前瞻性的方案讨论和技术调研。
【任职资格】
1、具备c++基础知识/熟悉汇编；
2、熟悉常规数据结构与算法，了解泛型编程（Template），具备一定的正向调试；
3、熟悉WinDBG、IDA Pro工具优先；
4、具备良好的编码规范素养，有逆向工程工作经验优先。
发，从网上了解到你们培训的学员
windows平台和android平台上的
经验但是在学校期间做过东西比较多
有机会解决户口。
工企业，想
和您那边合作！推荐人才！你方便时候
可以联系我！谢谢
本消息来自您的"QQ在线状态"，权限控
制请到官网: http://wp.qq.com
麦洛克菲内核，底层，安全
www.mallocfree.com

麦洛克菲内核，底层，安全

www.mallocfree.com


安全技术一瞥
麦洛克菲内核，底层，安全
www.mallocfree.com

API执行流程与文件过滤原理



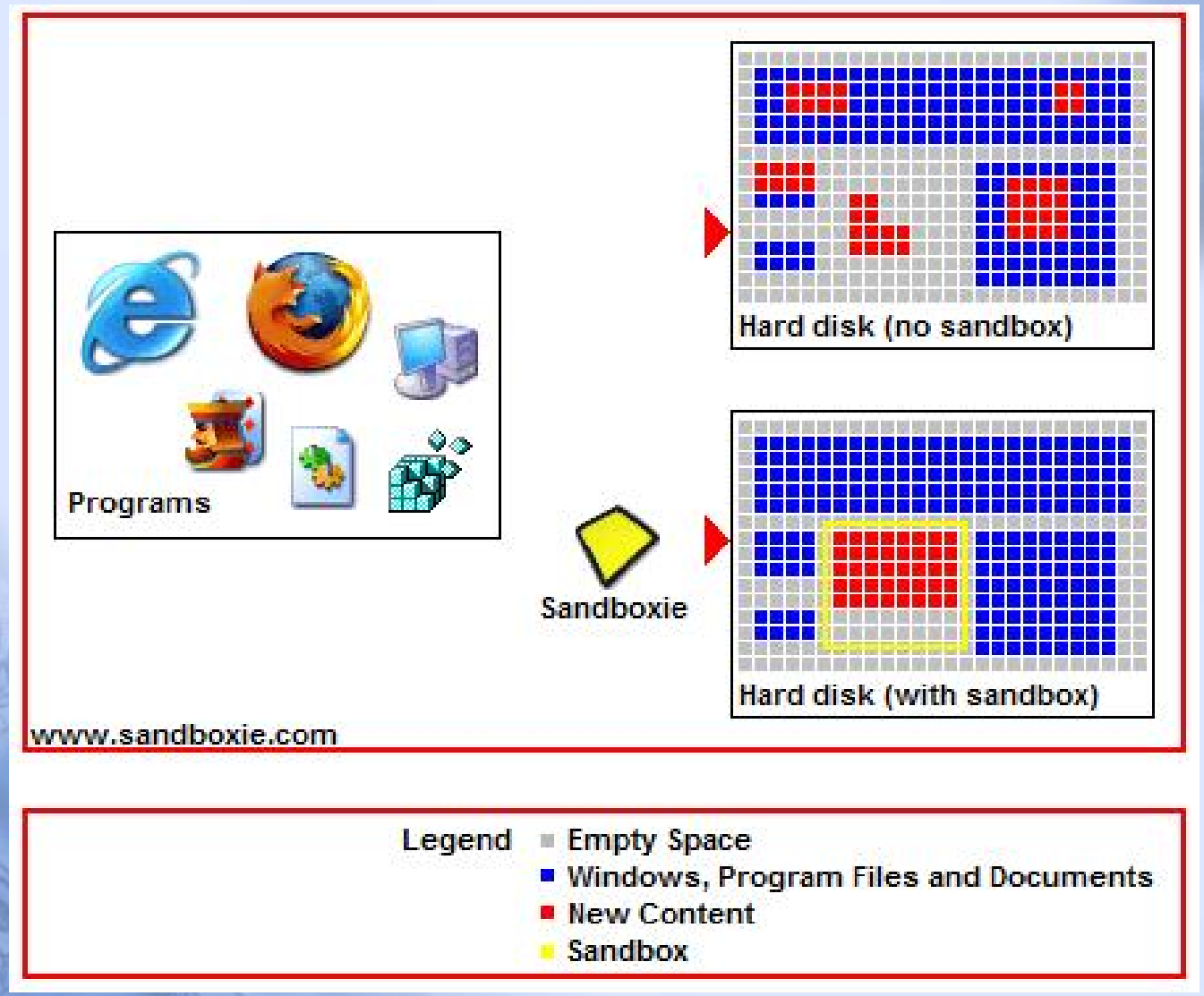
Hook
过滤
回调

主防，杀毒引擎，加解密软件，还原软件

麦[illegible]内核，底层，安全

[illegible]mallocfree.com

沙盘（Sandbox）技术



Rootkit与Anti-Rootkit技术

- Rootkit（RK 隐藏）
  - 进程
  - 文件
  - 注册表
  - 端口
  - 服务
- Anti-Rootkit （ARK）
  - Xuetr-PCHUNTER
  - Icesword
  - Darkspy
- Bootkit(手机bootkit)

逆向工程

- 反汇编工具IDA Pro
- 反C

```
int myFunc(int a, int b)
{
    int c = a + b;
    return c;
}
void main(void)
{
    int a = 0;
    int b = 1;
    myFunc(a, b);
}
```

a.Callee被调用者

```
mov     eax, dword ptr ss:[esp+8]
mov     ecx, dword ptr ss:[esp+4]
add     eax, ecx
ret
```

b.Caller调用者

```
push    1
push    0
call    MyFunc
add     esp,8
```

- 脱壳技术 vmp

Linux内核，移动安全Android

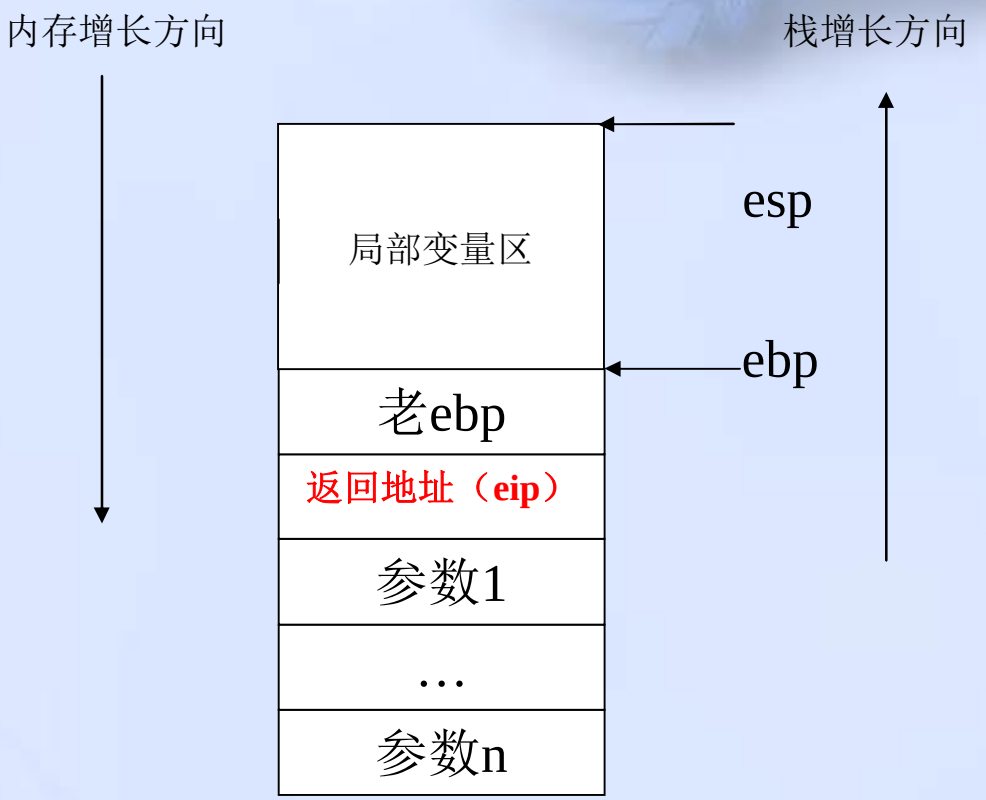
- 1.Java语言+Linux（NDK）
- 2.Android安全与病毒分析
- 3.SMALI语言，ARM汇编等

漏洞原理分析与挖掘

- 什么是漏洞？什么是0DAY和1DAY？
- 漏洞：能够导致软件做一些“超出设计范围的事情”的bug，叫漏洞。这类BUG，通常不会影响软件的正常功能，但如果被攻击者利用之后，会执行一些恶意的代码。
- 0Day：攻击者掌握的未被软件厂商修复的漏洞。
- POC代码：Proof of Concept，证明漏洞存在的代码
- cve.mitre.org/cert.org/blogs.360.cn/wooyun.org/freebuf.com

缓冲区溢出-栈溢出

```
void msg_display(char * buf)
{
    char msg[200];
    strcpy(msg,buf);
     cout<<msg<<endl;
}
```



缓冲区溢出—堆溢出

```
void func(char *buff)
{
   char *p1 = malloc( sizeof(node) ) ;
   strcpy( p1 , buff ) ; //溢出128+16个字节
   char *p2 = malloc( sizeof(node) ) ;
   //....
   return;
}
```

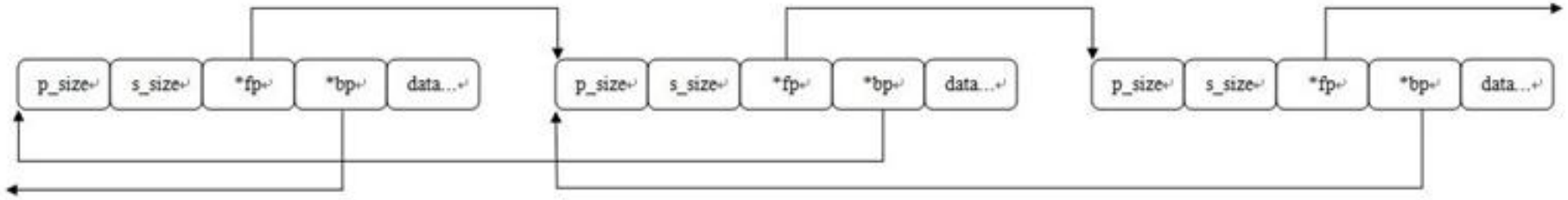
Node1->bp->fp = Node1->fp

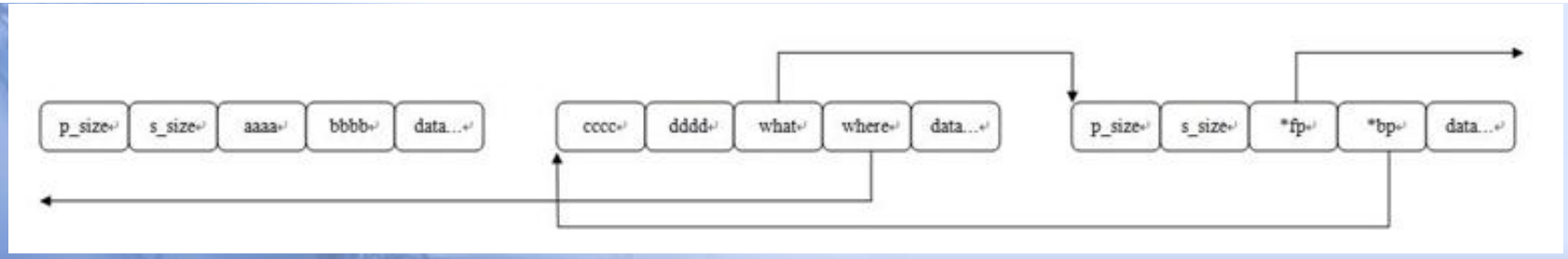
((Node1->where) + 0x8) = (Node1->what)

Node1->fp->bp = Node1->bp

((Node1->what) + 0xC) = (Node1->where)

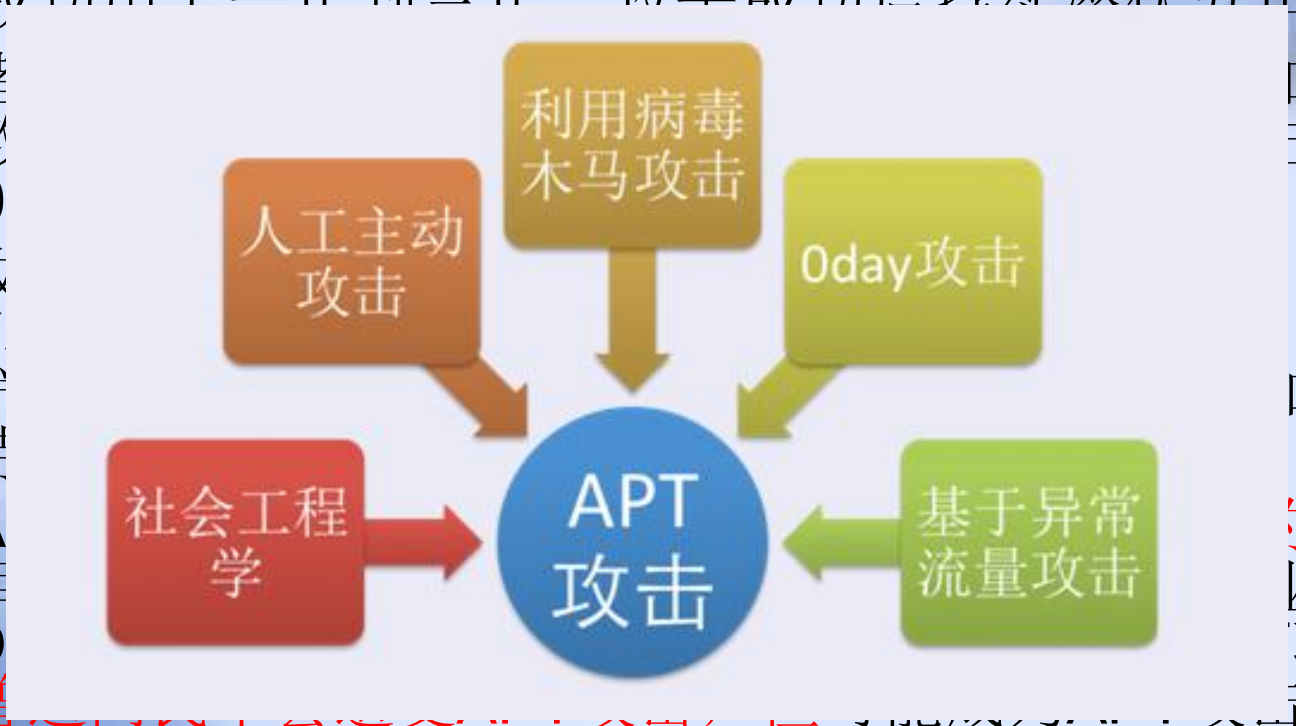
Node1





APT攻击

- APT:高级持续性威胁(Advanced Persistent Threat，APT)攻击
- 攻击成功用上一年到三年，攻击成功后持续潜伏五年到十年
- 攻击者
  个被攻
  发起0
- APT攻
  0DAY
  测对抗
  持的特
- 因此A
  一般军
  (GOO
  虽然普
  跳板
- 物理隔绝对APT攻击可能无效



APT攻击案例-极光攻击

- 针对GOOGLE等三十多个高科技公司。攻击者通过FACEBOOK上的好友分析，锁定了GOOGLE公司的一个员工和他的一个喜欢摄影的电脑小白好友。攻击者入侵并控制了电脑小白好友的机器，然后伪造了一个照片服务器，上面放置了IE的0DAY攻击代码，以电脑小白的身份给GOOGLE员工发送IM消息邀请他来看最新的照片，其实URL指向了这个IE 0DAY的页面。GOOGLE的员工相信之后打开了这个页面然后中招，攻击者利用GOOGLE这个员工的身份在内网内持续渗透，直到获得了GMAIL系统中很多敏感用户的访问权限。窃取了MAIL系统中的敏感信息后，攻击者通过合法加密信道将数据传出。事后调查，不止是GOOGLE中招了，三十多家美国高科技公司都被这一APT攻击搞定，甚至包括赛门铁克这样牛比的安全厂商

APT攻击案例-震网攻击stuxnet

- 伊朗核电站是一个物理隔离的网络，因此攻击者首先获得了一些核电站工作人员和其家庭成员的信息，针对这些家庭成员的主机发起了攻击，成功控制了这些家庭用的主机，然后利用4个WINDOWS的0DAY漏洞，**可以感染所有接入的USB移动介质以及通过USB移动介质可以攻击接入的主机**。终于靠这种摆渡攻击渗透进了防护森严物理隔离的伊朗核电站内部网络，最后再利用了3个西门子的0DAY漏洞，成功控制了控制离心机的控制系统，修改了离心机参数，让其发电正常但生产不出制造核武器的物质，但在人工检测显示端显示一切正常。成功的将伊朗制造核武器的进程拖后了几年。

学习安全资源推荐

学习安全技术重要参考

- 《一站式学习C编程》
- 《C语言编程精粹》 姜静波等译 电子工业
- 《高质量C++/C编程指南》 林锐 电子工业
- 《Effective C++》侯捷译 华中科技大学出版社
- 《More Effective C++》侯捷译 中国电力出版社

- 《汇编语言》 王爽 清华大学出版社
- 《天书夜读》 邵坚磊 电子工业出版社

- 《数据结构》 严尉敏 C语言版 清华大学
- 《数据结构习题与解析》 李春葆 C语言版

学习安全技术重要参考

- 《Windows 2000设备驱动程序设计指南》 Art Baker等著 施诺译 机械工业
- 《寒江独钓:Windows内核安全编程》 邵坚磊等著 电子工业出版社
- 《天书夜读:从汇编语言到Windows内核编程》邵坚磊等著 电子工业
- 《 Windows驱动开发技术详解》 张帆 电子工业出版社
- 《 Rootkits: Subverting the Windows Kernel 》 Greg Hoglund等著
- 《Windows NT File System Internals》

- 《0day安全：软件漏洞分析技术.第2版》 王清 电子工业出版社

- 《Android软件安全与逆向分析》
- 《Android安全攻防权威指南》

- 《UNIX环境高级编程第二版》
- 《Linux程序设计（第四版）》

- 《Linux设备驱动程序第三版》
- 《Linux内核设计与实现第三版》
- 《Linux设备驱动开发详解》

- 《Linux_内核完全注释_V11_赵炯》
- 《深入分析Linux内核源码》

学习安全技术重要参考

- 网站：
  - http://bbs.pediy.com
  - http://www.wooyun.org
  - http://www.freebuf.com/
  - cve.mitre.org
  - cert.org
  - blogs.360.cn
- 安全界领军人物：
  - Wowocock
  - Linxer
  - Mj0011
- 麦洛克菲：mallocfree.com 权威安全培训机构

如何求职IT名企：BAT

一份体现能力的简历

- 简历命名：姓名+学校+求职职位， 正文标题就写自己名字
- 简历包含内容：基本信息，教育经历，工作经历，项目经验，技能信息，个人作品（截图），个人技术博客地址，自我评价兴趣爱好等。倒叙。
- 简历要求：无错误，针对性强，扬长避短（突出最match的项目经验和技能，突出自己的成绩和优点）
- 一、二个精通，若干个熟练，若干个了解。篇幅1到2页
- 英语：band 6, be proficient in, be familiar with, skillful in use of, experience in, have a knowledge of

求职BAT等IT名企的方法论

- 基础知识点面试
- 算法面试
- 项目经验面试
- 外企：英语自我介绍，项目介绍，或者老外面试
- 优缺点介绍
- 期望薪水多少？如果给出薪水比期望低，还会考虑吗？
- 为什么选择来XXX工作？
- 精心的求职前准备，复习下项目和知识点
- 进入企业实习提高自己的经验
- 求职失败后，加强学习和经验积累，以退为进，持之以恒的决心。求职=能力+经验+学历+运气
- 专注于某一个领域，厚积薄发

求职BAT等IT名企的方法论

一，技术篇常见考点（技术是重点为大家集中详细培训的地方）

- C（如sizeof，static，整数存储，指针，位运算）
- C++(面向对象，构造函数，多态，STL库底层结构等）
- 内存管理：栈，堆，内存泄漏等
- 多线程/多进程：同步与互斥，通信方式等
- 数据结构与算法（如字符串相关算法）
- 网络协议（建立连接和断开连接的握手，定时器，MTU大小）
- 数据库： SQL编程，存储引擎，锁定等
- Windows系统：PE结构等
- Linux系统：CORE文件
- Android系统等
- 设计模式： Singleton单例模式，工厂模式，Adapter 模式

常见算法归纳总结与实战

- 2个指针跑步法
- 递归
- 熟练掌握循环
- 严进宽出
- 效率（时间空间复杂度）
- 边界考虑

礼物赠送环节：

- 《程序员求职成功路》
- 《IT求职笔试面试考点归纳》
- 如何获取：

QQ群：213774841：

QQ:10950150

验证信息:内核安全

官网： www.mallocfree.com

对进一步学习安全有兴趣的同学如何联系我们：

官网：www.mallocfree.com

预科QQ群：213774841

QQ:10950150

Q&A

The end