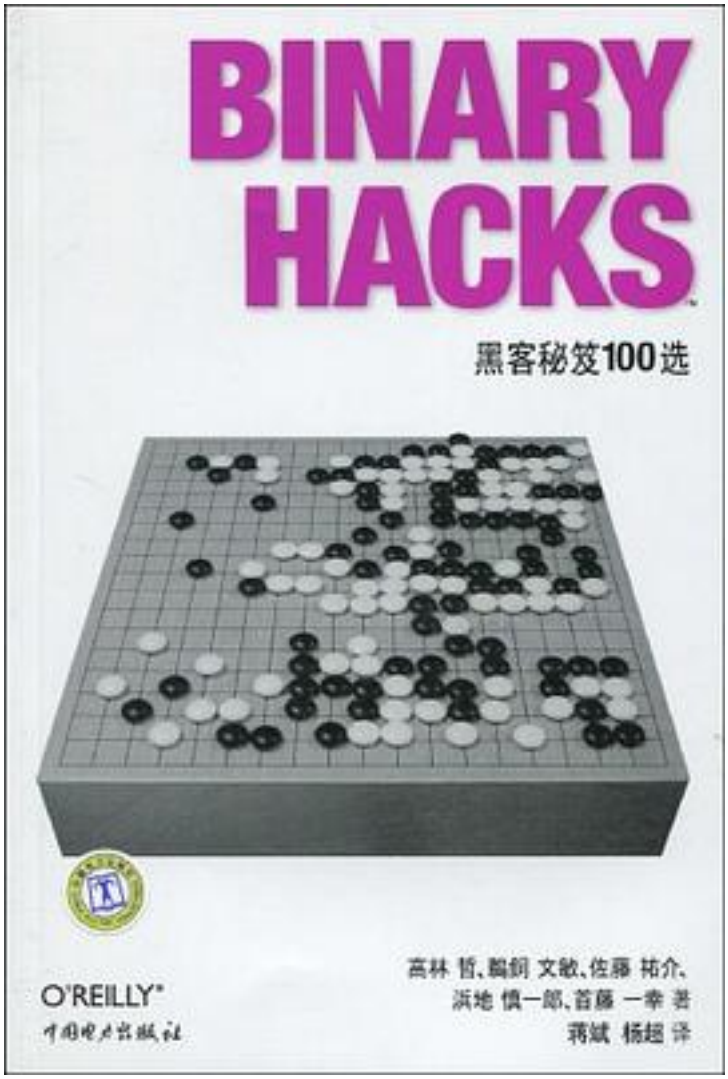
Binary Hacks



Binary Hacks_下载链接1_

著者:[日] 高林哲 等

出版者:

出版时间:2010-1

装帧:

isbn:9787508387932

《Binary Hacks:黑客秘笈100选》的主题是关于底层程序的技术。说到底层，就是和“原始的”计算机很接近的意思。软件的世界是一个抽象化的积累，逐步演化到现在的阶段。抽象化就是隐藏底层的复杂部分，相比较来说是可以提高生产性、安全性的方法，并给开发者提供程序化的手段。但是，如果认为完全不依赖底层系统级的技术来进行编程，这是行不通的。追求性能上的最佳，尽可能提高可信赖性，想解决偶尔发生的“谜一样的错误”，在这些情况下，了解底层系统级的技术就显得尤为重要。遗憾的是，抽象化并不能代替所有的。

《Binary Hacks:黑客秘笈100选》的目的就是在上述的情况下，都能使用的大量Know-how的介绍。《Binary Hacks:黑客秘笈100选》Binary Hack定义为“能驱动软件的底层技术的Know-how”，从最基本的工具使用开始，安全编程，OS到提高处理器的处理性能的技术，在一个很宽泛的范围内都进行了说明。

作者介绍:

目录: 本书寄语

30.在对外公开库的符号上利用版本来控制动作
31.在main()的前面调用函数
32.gcc根据生成的代码来生成运行时的代码
33.允许／禁止运行放置在stack里的代码
34.运行放置在heap上的代码
35.建成pie(位置独立运行形式)
36.用c++书写同步方法(synchronizedmethod)
37.用c++生成singleton
38.理解g++的异常处理(throw篇)
39.理解g++的异常处理(sjlj篇)
40.理解g++的异常处理(dwarf2篇)
41.理解g++异常处理的成本
第4章安全编程hack
42.gcc安全编写入门
43.用-ftrapv检测整数溢出
44.用mudflap检测出缓冲区溢出
45.用-d_fortify_source检测缓；中区溢出
46.用-fstack-protector保护堆栈
47.将进行位遮蔽的常量无符号化
48.注意避免移位过大
49.注意64位环境中0和null的不同之处
50.posix的线程安全函数
51.安全编写信号处理的方法
52.用sigwait将异步信号进行同步处理
53.用sigsafe将信号处理安全化
54.用valgrind检测出内存泄漏
55.使用valgrind检测出错误的内存访问
56.用helgrind检测出多线程程序的bug
57.用fakeroot在相似的root权限中运行进程
第5章运行时hack
58.程序转变成main()
59.怎样调用系统调用
60.用ld_preload更换共享库
61.用ld_preload来lap既存的函数
62.用dlopen进行运行时的动态链接
63.用c表示回溯
64.检测运行中进程的路径名
65.检测正在加载的共享库
66.掌握process和动态库mapmemory
67.用libbfd取得符号的一览表
68.运行c++语言时进行demangle
69.用ffcall动态决定签名，读出函数
70.用libdwarf取得调试信息
71.通过dumper简化dump结构体的数据
72.自行加载目标文件
73.通过libunwind控制call chain
74.用gnu lightning portable生成运行编码
75.获得stack的地址
76.用sigaltstack处理stack overflow
77.hook面向函数的enter／exit
78.从signal handler中改写程序的context
79.取得程序计数器的值
80.通过自动改写来改变程序的操作
81.使用sigsegv来确认地址的有效性

82.用strace来跟踪系统调用
83.用ltrace来跟踪进程调用共享库的函数
84.用jockey来记录，再生linux的程序运行
85.用prelink将程序启动高速化
86.通过livepatch在运行中的进程上发布补丁
第6章 profile调试器hack
87.使用gprof检索profile
88.使用sysprof搜索系统profile
89.使用oprofile获取详细的系统profile
90.使用gdb操作运行进程
91.使用硬件调试的功能
92.c程序中breakpoint的设定可以用断点这个说法
第7章 其他的hack
93.boehmgc的结构
94.请注意处理器的存储器顺序
95.对portable coroutine library(pcl)进行轻量的并行处理
96.计算cpu的clock数
97.浮点数的bit列表现
98.x86的浮点数运算命令的特殊性
99.用结果无限大和nan化运算来生成信号
100.文献介绍
・・・・・・(收起)

Binary Hacks_下载链接1_

标签

计算机

hacks

Linux

编程

binary

C/C++

程序设计

中文版

评论

翻译得很渣。linux上的一些编译链接技巧。其中不用libc生成binary那节现在有更精简的办法得到更小的可执行文件了。

翻译的太烂了。。

看在原作的份上给三星. 翻译实在是...

没有完全看完，主要是里面讲的大多数是比较偏的东西，平时不太会用到

原书的确是好书，但是中译本实在翻译的太烂。这里给4颗星完全是给原作者的。

同 debug hacks

很不错的书

个人基础不行,看得不是很懂

原书不错，估计只是翻译的错了，唉，毁书不倦~~

其实是一本非常好也非常实用的书，至于翻译问题，不是我见过翻译的最差的~

我跳着看, 翻译质量对我影响不大

不喜欢，太散

实在是很难理解的翻译。可以man 相关的命令，再练习一下，自己体会书中的例子。

原书四星；翻译一星，好多自造的术语

大部分看不懂

关于逆向的书。还没读，我也不知道自己会不会活到需要学习它的时候。

翻译太差 浪费时间 可惜日文看不懂，原版应该是本好书

HACKS系列好书之一。

翻译大垃圾。

翻译很烂，但是确实是一本不错的书。可作为debug时的一本工具书

Binary Hacks_下载链接1_

书评

我不会日语，所以把原书给我我也看不懂。这里只说中文版。今天刚拿到书，看第二章，ELF的规范我看过不止一遍，即使这样我也不知道第二章的前10页在说什么，或者说我很难把这些汉字和我看过的东西联系在一起，即便是我在大脑中进行"中文<--->英文"的转换之后。 这本书的中文用...

刚看到这本书的时候，欣喜啊，觉得又有一本经典的编程著作问世了。可是看了china-pub上的书评，听说这本书是用金山快译翻译的，有点不敢买了。
在很久以前，上中学的时候，有个老师告诉我们，要是作者在书里留下了联系方式，说明这个作者是一个负责的人，这样的书可以买，就算...

随便一翻，看到Hack100，文献。 严重怀疑作者没有相关行业背景， 详解Unix编程 应该是 Advanced Programing in the Unix Environment
国内翻译叫做Unix环境高级编程。 计算机的构成和设计, 应该是Computer Organization and Design. 国内翻译我记得是，计算机组织与设计 D...

翻译的实在太差，大量的句子不通顺、用词匪夷所思。很差，是给译者和编辑，大败O Reilly的牌子。书的内容对于学习了解Linux开发一些底层知识和技巧还是有价值的，我是把书中的内容作为索引在网上搜索自学的。 期待有负责的人士重新翻译出版。

内容非常好，翻译太**，作者居然还敢署名，看完想抽他。。。
出版社也不负责任，没有专业的审校吗。。。
翻译不好至少可以出个英文版嘛，现在也没得其它选择。。。 字数不够：
内容非常好，翻译太**，作者居然还敢署名，看完想抽他。。。
出版社也不负责任，没有专业的审校吗...

能翻译成这样也真不容易。 strtab被翻译成了“存储器表”。。。
还有一个“大范围脱溢”我愣是没听说过，估计是“widely unwinding”吧。。。
还有一砣连读都读不通的句子。。。 我靠!

作者：Satoru Takabayashi 出版社：O'Reilly Japan

《Binary Hacks》 作者：Satoru Takabayashi 出版社：O'Reilly Japan

《Binary
Hacks:黑客秘笈100选》的主题是关于底层程序的技术。说到底层，就是和“原始的”计算机很接近的意思。软件的世界是一个抽象化的积累，逐步演化到现在的阶段。抽象化就是隐藏底层的复杂部分，相比较来说是可以提高生产性、安全性的方法，并给开发者提供程序化的手段。...

本书在美国 amazon上的网页：
http://www.amazon.com/BINARY-HACKS-Tips-hackers-election/dp/7508387937/
看到了吗？ Author 是：GAO LIN ZHE (DENG) JIANG BIN YANG CHAO YI
太诡异了！ 狗屎翻译跟病毒一样，还具有传染性!

Binary Hacks_下载链接1_