

# 《黑客攻防技术宝典》

## 图书基本信息

书名：《黑客攻防技术宝典》

13位ISBN编号：9787115328489

10位ISBN编号：711532848X

出版时间：2013-9

出版社：人民邮电出版社

作者：[美]Charlie Miller,[美]Dionysus Blazakis,[美]Dino Dai Zovi,[美]Stefan Esser,[美]Vincenzo Iozzo,[美]Ralf-Philipp Weinmann

页数：320

译者：傅尔也

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《黑客攻防技术宝典》

## 内容概要

安全始终是计算机和互联网领域最重要的话题。进入移动互联网时代，移动平台和设备的安全问题更加突出。iOS系统凭借其在移动市场的占有率拥有着举足轻重的地位。虽然iOS系统向来以安全著称，但由其自身漏洞而引发的威胁同样一直存在。

《黑客攻防技术宝典：iOS实战篇》由美国国家安全局全球网络漏洞攻击分析师、连续4年Pwn2Own黑客竞赛大奖得主Charlie Miller领衔，6位业内顶级专家合力打造，全面深入介绍了iOS的工作原理、安全架构、安全风险，揭秘了iOS越狱工作原理，探讨了加密、代码签名、内存保护、沙盒机制、iPhone模糊测试、漏洞攻击程序、ROP有效载荷、基带攻击等内容，为深入理解和保护iOS设备提供了足够的知识与工具，是学习iOS设备工作原理、理解越狱和破解、开展iOS漏洞研究的重量级专著。

本书作为国内第一本全面介绍iOS漏洞及攻防的专著，作者阵容空前豪华，内容权威性毋庸置疑。

Charlie Miller曾在美国国家安全局担任全球网络漏洞攻击分析师5年，并连续4届摘得Pwn2Own黑客竞赛桂冠。Dionysus Blazakis擅长漏洞攻击缓解技术，2010年赢得了Pwnie Award最具创新研究奖。Dino Dai Zovi是Trail of Bits联合创始人和首席技术官，有十余年信息安全领域从业经验，出版过两部信息安全专著。Vincenzo Iozzo现任BlackHat和Shakacon安全会议评审委员会委员，因2010年和2011年连续两届获得Pwn2Own比赛大奖在信息安全领域名声大振。Stefan Esser是业界知名的PHP安全问题专家，是从原厂XBOX的硬盘上直接引导Linux成功的第一人。Ralf-Philipp Weinmann作为德国达姆施塔特工业大学密码学博士、卢森堡大学博士后研究员，对密码学、移动设备安全等都有深入研究。

本书适合想了解iOS设备工作原理的人，适合对越狱和破解感兴趣的人，适合关注iOS应用及数据安全的开发人员，适合公司技术管理人员（他们需要了解如何保障iOS设备安全），还适合从事iOS漏洞研究的安全研究人员。

## 作者简介

### Charlie Miller

Accuvant Labs首席研究顾问，曾在美国国家安全局担任全球网络漏洞攻击分析师5年，连续4年赢得CanSecWest Pwn2Own黑客大赛。他发现了iPhone与G1安卓手机第一个公开的远程漏洞，通过短信对iPhone进行漏洞攻击并发现了可以让恶意软件进入iOS的代码签名机制缺陷。作为圣母大学博士的他还与人合著了The Mac Hacker's Handbook和Fuzzing for Software Security Testing and Quality Assurance两本信息安全类图书。

### Dionysus Blazakis

程序员和安全研究人员，擅长漏洞攻击缓解技术，经常在安全会议上发表有关漏洞攻击缓解技术、绕过缓解技术和寻找漏洞的新方法等主题演讲，因利用即时编译器绕过数据执行保护的技术赢得了2010年Pwnie Award最具创新研究奖。另外，他与Charlie Miller为参加2011年Pwn2Own大赛开发的iOS漏洞攻击程序赢得了iPhone漏洞攻击比赛的大奖。

### Dino Dai Zovi

Trail of Bits联合创始人和首席技术官，有十余年信息安全领域从业经验，做过红队（red teaming，又称“伦理黑客”）、渗透测试、软件安全、信息安全管理与网络安全研究与开发等多种工作。Dino是信息安全会议的常客，在DEFCON、BlackHat和CanSecWest等世界知名的信息安全会议上发表过对内存损坏利用技术、802.11无线客户端攻击和英特尔VT-x虚拟化rootkit程序等课题的独立研究成果。他还是The Mac Hacker's Handbook和The Art of Software Security Testing的合著者。

### Vincenzo Iozzo

Tiqad srl安全研究人员，BlackHat和Shakacon安全会议评审委员会成员，常在BlackHat和CanSecWest等信息安全会议上发表演讲。他与人合作为BlackBerryOS和iPhoneOS编写了漏洞攻击程序，因2010年和2011年连续两届获得Pwn2Own比赛大奖在信息安全领域名声大振。

### Stefan Esser

因在PHP安全方面的造诣为人熟知，2002年成为PHP核心开发者以来主要关注PHP和PHP应用程序漏洞的研究，早期发表过很多关于CVS、Samba、OpenBSD或Internet Explorer等软件中漏洞的报告。2003年他利用了XBOX字体加载器中存在的缓冲区溢出漏洞，成为从原厂XBOX的硬盘上直接引导Linux成功的第一人；2004年成立Hardened-PHP项目，旨在开发更安全的PHP，也就是Hardened-PHP（2006年融入Suhosin PHP安全系统）；2007年与人合办德国Web应用开发公司SektionEins GmbH并负责研发工作；2010年起积极研究iOS安全问题，并在2011年提供了一个用于越狱的漏洞攻击程序（曾在苹果多次更新后幸存下来）。

### Ralf-Philipp Weinmann

德国达姆施塔特工业大学密码学博士、卢森堡大学博士后研究员。他在信息安全方面的研究方向众多，涉及密码学、移动设备安全等很多主题。让他声名远播的事迹包括参与让WEP破解剧烈提速的项目、分析苹果的FileVault加密、擅长逆向工程技术、攻破DECT中的专属加密算法，以及成功通过智能手机的Web浏览器（Pwn2Own）和GSM协议栈进行渗透攻击。

## 书籍目录

### 目录

第1章 iOS安全基础知识	1
1.1 iOS硬件/设备的类型	1
1.2 苹果公司如何保护App Store	2
1.3 理解安全威胁	3
1.4 理解iOS的安全架构	4
1.4.1 更小的受攻击面	4
1.4.2 精简过的iOS	5
1.4.3 权限分离	5
1.4.4 代码签名	5
1.4.5 数据执行保护	6
1.4.6 地址空间布局随机化	6
1.4.7 沙盒	6
1.5 iOS攻击简史	7
1.5.1 Libtiff	7
1.5.2 短信攻击	8
1.5.3 Ikee蠕虫	8
1.5.4 Storm8	9
1.5.5 SpyPhone	10
1.5.6 Pwn2Own 2010	10
1.5.7 Jailbreakme.com 2 ( “ Star ” )	10
1.5.8 Jailbreakme.com 3 ( “ Saffron ” )	11
1.6 小结	11
第2章 企业中的iOS	12
2.1 iOS配置管理	12
2.1.1 移动配置描述文件	13
2.1.2 iPhone配置实用工具	14
2.2 移动设备管理	21
2.2.1 MDM网络通信	21
2.2.2 Lion Server描述文件管理器	22
2.3 小结	36
第3章 加密	37
3.1 数据保护	37
3.2 对数据保护的攻击	40
3.2.1 对用户密码的攻击	40
3.2.2 iPhone Data Protection Tools	43
3.3 小结	54
第4章 代码签名和内存保护	55
4.1 强制访问控制	56
4.1.1 AMFI钩子	56
4.1.2 AMFI和execv	57
4.2 授权的工作原理	59
4.2.1 理解授权描述文件	59
4.2.2 如何验证授权文件的有效性	62
4.3 理解应用签名	62
4.4 深入了解特权	64

4.5	代码签名的实施方法	65	
4.5.1	收集和验证签名信息	65	
4.5.2	如何在进程上实施签名	68	
4.5.3	iOS如何确保已签名页不发生改变	72	
4.6	探索动态代码签名	73	
4.6.1	MobileSafari的特殊性	73	
4.6.2	内核如何处理即时编译	75	
4.6.3	MobileSafari内部的攻击	77	
4.7	破坏代码签名机制	78	
4.7.1	修改iOS shellcode	79	
4.7.2	在iOS上使用Meterpreter	83	
4.7.3	取得App Store的批准	85	
4.8	小结	86	
第5章	沙盒	87	
5.1	理解沙盒	87	
5.2	在应用开发中使用沙盒	89	
5.3	理解沙盒的实现	95	
5.3.1	理解用户空间库的实现	95	
5.3.2	深入内核	98	
5.3.3	沙盒机制对App Store应用和平台应用的影响	109	
5.4	小结	113	
第6章	对iOS应用进行模糊测试	114	
6.1	模糊测试的原理	114	
6.2	如何进行模糊测试	115	
6.2.1	基于变异的模糊测试	116	
6.2.2	基于生成的模糊测试	116	
6.2.3	提交和监测测试用例	117	
6.3	对Safari进行模糊测试	118	
6.3.1	选择接口	118	
6.3.2	生成测试用例	118	
6.3.3	测试和监测应用	119	
6.4	PDF模糊测试中的冒险	122	
6.5	对快速查看 ( Quick Look ) 的模糊测试	126	
6.6	用模拟器进行模糊测试	127	
6.7	对MobileSafari进行模糊测试	130	
6.7.1	选择进行模糊测试的接口	130	
6.7.2	生成测试用例	130	
6.7.3	MobileSafari的模糊测试与监测	131	
6.8	PPT模糊测试	133	
6.9	对SMS的模糊测试	134	
6.9.1	SMS基础知识	135	
6.9.2	聚焦协议数据单元模式	136	
6.9.3	PDUspy的使用	138	
6.9.4	用户数据头信息的使用	139	
6.9.5	拼接消息的处理	139	
6.9.6	其他类型UDH数据的使用	139	
6.9.7	用Sulley进行基于生成的模糊测试	141	
6.9.8	SMS iOS注入	145	
6.9.9	SMS的监测	146	

6.9.10	SMS bug	151
6.10	小结	153
<b>第7章 漏洞攻击 154</b>		
7.1	针对bug类的漏洞攻击	154
7.2	理解iOS系统自带的分配程序	156
7.2.1	区域	156
7.2.2	内存分配	157
7.2.3	内存释放	157
7.3	驯服iOS的分配程序	158
7.3.1	所需工具	158
7.3.2	与分配/释放有关的基础知识	159
7.4	理解TCMalloc	167
7.4.1	大对象的分配和释放	167
7.4.2	小对象的分配	168
7.4.3	小对象的释放	168
7.5	驯服TCMalloc	168
7.5.1	获得可预知的堆布局	168
7.5.2	用于调试堆操作代码的工具	170
7.5.3	堆风水：以TCMalloc对算术漏洞进行攻击	172
7.5.4	以TCMalloc就对象生存期问题进行漏洞攻击	175
7.6	对ASLR的挑战	176
7.7	案例研究：Pwn2Own 2010	177
7.8	测试基础设施	181
7.9	小结	181
<b>第8章 面向返回的程序设计 182</b>		
8.1	ARM基础知识	182
8.1.1	iOS的调用约定	183
8.1.2	系统调用的调用约定	183
8.2	ROP简介	185
8.2.1	ROP与堆bug	186
8.2.2	手工构造ROP有效载荷	187
8.2.3	ROP有效载荷构造过程的自动化	191
8.3	在iOS中使用ROP	193
8.4	iOS中ROP shellcode的示例	195
8.4.1	用于盗取文件内容的有效载荷	196
8.4.2	利用ROP结合两种漏洞攻击程序 ( JailBreakMe v3 )	202
8.5	小结	206
<b>第9章 内核的调试与漏洞攻击 207</b>		
9.1	内核的结构	207
9.2	内核的调试	208
9.3	内核扩展与IOKit驱动程序	213
9.3.1	对IOKit驱动程序对象树的逆向处理	213
9.3.2	在内核扩展中寻找漏洞	216
9.3.3	在IOKit驱动程序中寻找漏洞	219
9.4	内核漏洞攻击	222
9.4.1	任意内存的重写	223
9.4.2	未初始化的内核变量	227
9.4.3	内核栈缓冲区溢出	231
9.4.4	内核堆缓冲区溢出	236

9.5	小结	245
第10章	越狱	246
10.1	为何越狱	246
10.2	越狱的类型	247
10.2.1	越狱的持久性	247
10.2.2	漏洞攻击程序的类型	248
10.3	理解越狱过程	249
10.3.1	对bootrom进行漏洞攻击	250
10.3.2	引导ramdisk	250
10.3.3	为文件系统越狱	250
10.3.4	安装完美越狱漏洞攻击程序	251
10.3.5	安装AFC2服务	251
10.3.6	安装基本实用工具	252
10.3.7	应用转存	253
10.3.8	应用包安装	254
10.3.9	安装后的过程	255
10.4	执行内核有效载荷和补丁	255
10.4.1	内核状态修复	255
10.4.2	权限提升	256
10.4.3	为内核打补丁	257
10.4.4	安全返回	267
10.5	小结	268
第11章	基带攻击	269
11.1	GSM基础知识	270
11.2	建立OpenBTS	272
11.2.1	硬件要求	272
11.2.2	OpenBTS的安装和配置	273
11.3	协议栈之下的RTOS	276
11.3.1	Nucleus PLUS	276
11.3.2	ThreadX	277
11.3.3	REX/OKL4/Iguana	277
11.3.4	堆的实现	278
11.4	漏洞分析	281
11.4.1	获得并提取基带固件	281
11.4.2	将固件镜像载入IDA Pro	283
11.4.3	应用/基带处理器接口	283
11.4.4	栈跟踪与基带核心转储	283
11.4.5	受攻击面	284
11.4.6	二进制代码的静态分析	285
11.4.7	由规范引路的模糊测试	285
11.5	对基带的漏洞攻击	286
11.5.1	本地栈缓冲区溢出：AT+XAPP	286
11.5.2	ultrasn0w解锁工具	287
11.5.3	空中接口可利用的溢出	293
11.6	小结	299
附录	参考资料	300

# 《黑客攻防技术宝典》

## 精彩短评

- 1、强
- 2、译得烂死了。
- 3、图书馆
- 4、iOS上的黑客书，不过没开发过什么应用读起来有点吃力
- 5、4/13，拿去图书漂流了
- 6、任何的安全 接触到物理层面都没有安全可言 随着互联网的发生将有可能通过互联网来接触物理层面；
- 7、内力不够，曰，弃之。



# 《黑客攻防技术宝典》

## 精彩书评

1、1、翻译质量着实不敢恭维，很多是直译的。由于英文经常习惯用长句，如果直译成中文就会变得很绕口，完全不符合国人的表达思维。英译中就该把长句变短句，否则单纯从语义表面上看都相当费劲，更不用说技术层面了。比如下面这句：“其它代码可能调用xx以调用xx函数中的函数，如果你调用原始xx，就会因为副本xx未更新造成一致性问题”，真的很绕口。2、书中不少专业术语翻译不到位，比如“return-into-libc”利用技术居然被翻译成“返回libc中”，还有其它不少地方也是如此，表达上不过明确，可见译者对软件安全技术的不熟悉。3、书中有少表达不明确的地方，还有笔误，这种即使是非技术人员应该也是可以看出来，说明编辑审稿不严格，双方均有责任。

2、本书看了三分之一，对里面介绍的一些技术，文字意思到能理解，但一些基础代码和基础函数就比较难以理解！边看边百度搜索一些专业术语，进度挺慢！里面有个专业术语，一直没怎么弄明白，“ROP有效载荷”这个东西，不知道是什么，百度上说的是“信息数据元什么的”，还是不理解T\_T

# 《黑客攻防技术宝典》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu111.com](http://www.tushu111.com)