<<iOS应用安全攻防>>

图书基本信息

书名：<<iOS应用安全攻防>>

13位ISBN编号：9787564134464

10位ISBN编号：7564134461

出版时间：2012-6

出版时间：东南大学出版社

作者：扎德尔斯基

页数：336

字数：436000

<<iOS应用安全攻防>>

内容概要

如果你是一位具有坚实Objective-C基础的应用开发者，这本《iOS应用安全攻防(影印版)》绝对急你所需——你所在公司的iOS应用被攻击的可能性很大。
这是因为恶意攻击者现在使用一系列工具采用大多数程序员想象不到的方式进行反向工程、跟踪和操纵应用。

这本书讲解了几种iOS的攻击手段，以及黑客们常用的工具和技术。
你会从中学到保护你的应用的最佳方式，并且意识到像你的对手那样去理解和制定策略是多么重要。
本书由扎德尔斯基(Zdziarski,
J.)著。

作者简介

作者：（美国）扎德尔斯基（Jonathan Zdziarski）

<<iOS应用安全攻防>>

书籍目录

章节摘录

版权页： 插图： $ sudo port install cmake libusb-devel libplist Once these packages are installed, create a symlink for the libusb.h prototype so that the usbmuxd package can find it: Download and extract the contents of the usbmuxd source package: Use the cmake command to generate make files, then build the project with make: With usbmuxd installed, and its companion tool iproxy, you'll be able to establish the needed connection bridge from your desktop to your device. While iproxy comes with an open source implementation of usbmuxd, iTunes also includes an officially sanc tioned version from Apple that is much faster.To use the much faster version of usbmuxd included with iTunes, ensure that Apple's usbmuxd is loaded and then run the iproxy tool to establish a connection between a local machine (we'll arbitrarily use port 7777 here), and the echo port (port 7) on the device, which is the TCP port your payload code is listening on. $ sudo lauhchctl load /System/Library/LaunchDaemons/com.apple.usbmuxd.plist $ iproxy 7777 7 Once the proxy has started, use netcat (often invoked through its abbreviation nc) to connect to the device through localhost. The netcat utility is a simple tool to make (or listen for) arbitrary network connections, and send or receive data, $ nc 127.0.0,1 7777 > filesystem,tar The call to nc causes it to connect to the localhost on TCP port 7777. If the proxy and usbmux protocol are working, this connection will be tunneled across USB to the device on port 7, which you specified when you started iproxy. If the connection is working,you should see the device report to the screen that it is sending the/private filesystem,and will see thefilesystem.tar file grow on your desktop machine. When the transfer is finished, nc will exit and you will have the complete live user filesystem stored in filesystem.tar! Sometimes, iTunes may not have been properly installed, and you may have problems transferring data from the device. If the tar file remains a zero byte size, try unloading iTunes' copy of usbmuxd and running the open source version you just built.

<<iOS应用安全攻防>>

编辑推荐

《iOS应用安全攻防(影印版)(英文)》由扎德尔斯基著。
检查现实应用中的微小漏洞——并丑避免在你的应用中出现同样的问题，了解黑客如何通过代码注入来使应用感染恶意软件，明白攻击者如何破解iOS keychain和数据保护加密，使用调试器和定制代码注入来操纵运行时Objective—C环境，阻止攻击者劫持SSL会话和窃取数据流量，安全地删除文件和设计应用来防止数据泄露，避免滥用调试，验证运行时类的健全性，确保你的代码难以跟踪。

<<iOS应用安全攻防>>

版权说明